PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-282105
(43)Date of publication of application : 12.10.2001

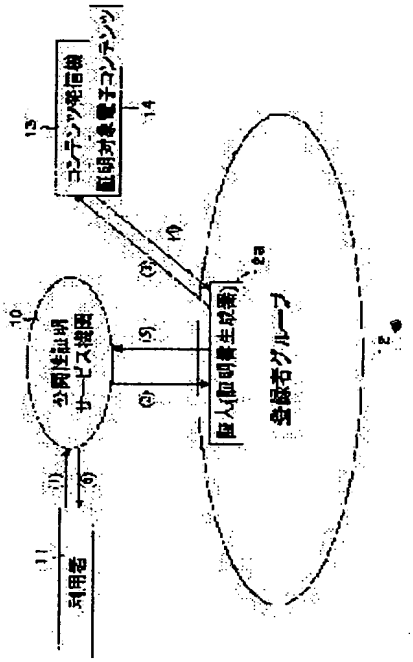
(51)Int.Cl. G09C 1/00
G06F 15/00
H04L 9/32

(21)Application number : 2000-087634
(22)Date of filing : 27.03.2000

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : NOGUCHI TETSUYA
KOYANAGI MITSUO
KAJIMA HISATSUGU

(54) CERTIFICATION METHOD FOR ELECTRONIC CONTENTS, SYSTEM AND MEDIUM WITH RECORDED PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To enhance ability of the publicity and the non-alterability property of electronic contents by giving evidence to the publicity of the electronic contents existing on a network.
SOLUTION: A service machine 10 chooses preferably plural witnesses from among register group 12 or a certificate generator 12a with respect to the service request of a user 11 wanting to have the testimony of the publicity of electronic contents and asks the witnesses or the certificate generator 12a to prepare the acquisition certificate of the electronic contents 14. Electronic signatures of the witnesses or the certificate generator 12a are attached to a certificate and the service machine 10 transmits this certificate to a user 11 after attaching, in addition, an electronic signature of his own.



LEGAL STATUS

[Date of request for examination] 11.01.2001
[Date of sending the examiner's decision of rejection] 21.07.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision

of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－282105
（P2001－282105A）
(43)公開日　平成13年10月12日(2001.10.12)

(51)Int.Cl.'	識別記号	Ｆ Ｉ	テーマコード'（参考）
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ　５Ｂ０８５
	６６０		６６０Ｅ　５Ｊ１０４
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ａ　９Ａ００１
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ

審査請求　有　　請求項の数20　ＯＬ　（全 28 頁）

(21)出願番号　特願2000－87634(P2000－87634)

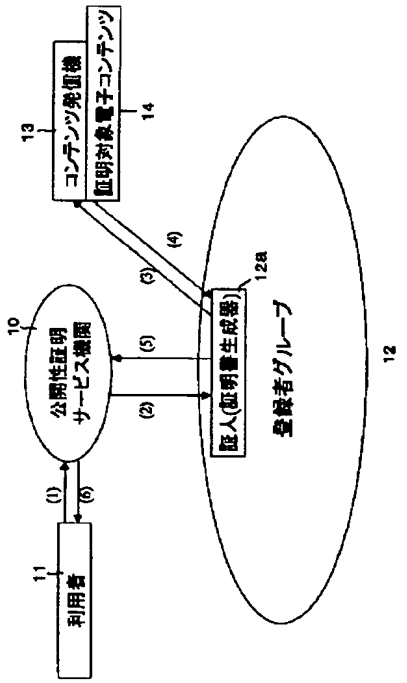
(22)出願日　平成12年３月27日(2000.3.27)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）
(74)復代理人　100112520
弁理士　林　茂則　（外２名）

最終頁に続く

(54)【発明の名称】　電子コンテンツの証明方法、システムおよびプログラムが記録された媒体

(57)【要約】
【課題】　ネットワーク上に存在する電子コンテンツの公開性を証拠付け、電子コンテンツの公開性あるいは不改変性の証拠能力を高める。
【解決手段】　電子コンテンツの公開性の証明を希望する利用者１１のサービス要求に対し、サービス機関１０が、登録者グループ１２の中から好ましくは複数の証人または証明書生成器１２ａを選抜し、前記証人または証明書生成器１２ａに電子コンテンツ１４の取得証明書の作成要求を出す。証明書には、証人または証明書生成器１２ａの電子署名が付され、サービス機関１０はさらにこの証明書に自己の電子署名を付して利用者１１に送付する。



1

【特許請求の範囲】

【請求項１】　コンピュータシステムまたはコンピュータネットワークを利用した電子コンテンツを証明する方法であって、

（ａ）前記証明のサービス機関が、証人または証明書生成器に対し、証明書作成要求を送信するステップと、

（ｂ）前記証人または証明書生成器が、前記サービス機関の証明書作成要求に応じて、前記電子コンテンツを取得するステップと、

（ｃ）証明書を作成するステップと、

を含む電子コンテンツの証明方法。

【請求項２】　前記証明書には、前記電子コンテンツまたは前記電子コンテンツを一義的に表すデータを含む請求項１記載の証明方法。

【請求項３】　前記証明方法には、さらに、

（ｄ）前記証明書が、前記サービス機関に蓄積されるステップまたは前記利用者に送付されるステップを含む請求項１または２記載の証明方法。

【請求項４】　前記証明書には、前記電子コンテンツのアドレス情報および前記証明の時刻情報を含む請求項１～３の何れか一項に記載の証明方法。

【請求項５】　前記証明書の作成ステップには、前記証明書に署名するステップを含み、前記署名ステップには、前記証人または証明書生成器による第１の署名ステップと、前記サービス機関による第２の署名ステップとを含む第１の構成、または、公証人サービス機関による署名ステップを含む第２の構成、の何れかの構成を有する請求項１～４の何れか一項に記載の証明方法。

【請求項６】　前記署名には、公開鍵暗号方式による暗号化を用い、署名者以外の改変を不可能とした請求項５記載の証明方法。

【請求項７】　前記電子コンテンツを一義的に表すデータが、ハッシュコードである請求項２～６の何れか一項に記載の証明方法。

【請求項８】　前記証明書作成要求は、前記利用者の要求に応じて、単一もしくは複数の期日に、または、単一もしくは複数の期間を定めて継続的に、前記証人または証明書生成器に送信される請求項１～７の何れか一項に記載の証明方法。

【請求項９】　前記サービス機関と前記証人または証明書生成器との間の時刻は、同期がとられる請求項１～８の何れか一項に記載の証明方法。

【請求項１０】　コンピュータシステムまたはコンピュータネットワークを利用した電子コンテンツを証明するシステムであって、

証人または証明書生成装置に対し証明書作成要求を送信する手段と、

前記証明書作成要求に応じて前記電子コンテンツを取得する手段と、

証明書を作成する手段と、

2

を備えた電子コンテンツの証明システム。

【請求項１１】　前記証明書には、前記電子コンテンツまたは前記電子コンテンツを一義的に表すデータを含む請求項１０記載の証明システム。

【請求項１２】　前記証明システムには、さらに、

前記証明書を、前記サービス機関のコンピュータシステムに蓄積する手段または前記利用者に送付する手段の何れかを備えた請求項１０または１１記載の証明システム。

【請求項１３】　前記証明書には、前記電子コンテンツのアドレス情報および前記証明の時刻情報が含まれる請求項１０～１２の何れか一項に記載の証明システム。

【請求項１４】　前記証明書の作成手段には、前記証明書に署名する手段を含み、前記署名手段には、前記証人または証明書生成器による第１の署名手段と、前記サービス機関による第２の署名手段とを含む第１の構成、または、公証人サービス機関による署名手段を含む第２の構成、の何れかの構成を有する請求項１０～１３の何れか一項に記載の証明システム。

【請求項１５】　前記署名手段には公開鍵暗号方式による暗号化手段を用い、署名者以外の改変を不可能とした請求項１４記載の証明システム。

【請求項１６】　コンピュータシステムまたはコンピュータネットワークを利用した電子コンテンツの公開性または不改変性を証明するサービス機関のシステムであって、

利用者のサービス要求を受理し、前記サービス要求を解析する手段と、

証人または証明書生成器が、登録された登録者グループから、前記証人または証明書生成器を選出する手段と、

前記証人または証明書生成器に証明書作成要求を送信する手段と、

前記証人または証明書生成器から返送された証明書を受理する手段と、

前記証明書を前記利用者に送信する手段とを備えた前記サービス機関の証明システム。

【請求項１７】　前記証明書の受理手段には、前記証明書に電子署名を施す手段が含まれる請求項１６記載のシステム。

【請求項１８】　コンピュータシステムまたはコンピュータネットワークを利用した電子コンテンツの公開性または不改変性を証明する証人または証明書生成器のシステムであって、

サービス機関からの証明書作成要求を受理する手段と、

前記証明書作成要求に含まれる前記電子コンテンツのアドレスにアクセスし、前記電子コンテンツを取得する手段と、

前記電子コンテンツまたは前記電子コンテンツを一義的に表すコードを含む証明書を作成する手段と、

前記証明書を前記サービス機関に返信する手段と、

を備えた前記証人または証明書生成器のシステム。

【請求項１９】　前記証明書の作成手段には、前記証明書に電子署名を施す手段が含まれる請求項１８記載のシステム。

【請求項２０】　コンピュータシステムまたはコンピュータネットワークを利用した電子コンテンツの公開性または不改変性を証明するプログラムコードが記録された媒体であって、前記プログラムコードには、

利用者または自己のサービス要求に応じて、証人または証明書生成装置に対し、証明書作成要求を送信するプログラムコードと、

前記サービス機関の証明書作成要求に応じて、前記電子コンテンツを取得するプログラムコードと、

前記電子コンテンツまたは前記電子コンテンツを一義的に表すデータを含む証明書を作成するプログラムコードと、

前記証明書を、前記サービス機関のコンピュータシステムに蓄積するプログラムコードまたは前記利用者に送付するプログラムコードの何れかと、

を含むプログラムコードが記録された媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子コンテンツの証明方法、システムおよびプログラムが記録された媒体に関し、特に、電子コンテンツの公開性、不改変性の証明に適用して有効な技術に関する。

【０００２】

【従来の技術】従来、思想感情等の表白あるいは発明等技術思想の公表、その他公開されるべきあらゆる文書図面等の情報は、紙媒体に文字・図形等を印刷した印刷物あるいは出版物として公開されるのが一般的である。このような印刷物は、裁判上の書証として扱われるほか、自由な契約を行える二者間の証拠書類、行政手続上の証拠書類、たとえば特許法における新規性喪失の証拠書類（特許法２９条１項３号、３０条等）として扱われる。印刷物あるいは出版物の場合、その存在あるいは公開の事実は、出版物等とその出版日を証明して立証できる。また、出版物等の改変は通常明瞭に見分けることができるため、それが改変されていないことを証明して不改変性の立証も行える。

【０００３】一方、インターネット等近年の情報技術の進展に伴い、従来、印刷物等により公開されていた情報（コンテンツ）が電子コンテンツとしてネットワーク上で公開される機会が増加している。このような電子コンテンツにあっても、印刷物と同様にコンテンツ（情報）が開示される以上、前記したような証拠として活用したいという要求が存在する。

【０００４】電子コンテンツの存在を立証する手法としては、たとえば「www.surety.com」等の電子公証人システムが知られている。このような電子公証人システムで

は、電子コンテンツの内容をハッシュコード等に変換して、前記ハッシュコードを新聞等に発表して不特定の第三者に前記コンテンツの存在を知らしめ、電子コンテンツが存在する事実を立証する。これにより、電子コンテンツに記載の事実の立証が可能になり、たとえば電子コンテンツに著作物が含まれるようなときには著作権の発生等を立証することが可能となる。

【０００５】ところが、電子コンテンツを前記したような証拠として活用しようとした場合、出版物とは相違する特有の問題、つまりコンテンツの証明力の問題がある。電子コンテンツの場合、一般的にはホームページ等へのアップロードは公開者（ホームページ作成者）により自主的に行われるため、公開内容および公開日の証明は公証機関等第三者による証明がなければ立証が困難である。また、ホームページ等の運営は一般的には自主的に行われるため、コンテンツの改変はホームページ運営者により自由に行うことができ、コンテンツの不改変性についても第三者の公証がなければ証拠力が弱いと考えられる。前記した通り電子コンテンツの存在性を立証する手段は既に存在するが、電子コンテンツの存在を立証するだけでは印刷物の証拠力に匹敵する証拠力を得ることはできない。たとえば電子コンテンツ記載の技術思想（発明）が特許法２９条１項３号の「電気通信回線を通じて公衆に利用可能となった発明」に該当するためには、特許庁による「インターネット等の情報の先行技術としての取り扱い運用指針」によれば、情報が「公衆に利用可能」であること、つまり、不特定の者に見得るような状態におかれることを要し、また、出願前において引用する電子的技術情報がその内容のとおりに掲載されていたことを要する。しかしながら前記した従来技術では公開性（公衆の利用可能性）は立証されず、また、出願時における不改変性を立証することはできない。

【０００６】また、前記した特許法における先行技術の場合に限らず、電子コンテンツの公開性（公衆性）および不改変性を立証したい場合がある。しかし、前記した従来技術では、特定の日時に特定の内容の電子コンテンツが存在したことが立証されるに止まり、その公開性、不改変性（完全性、正当性）の立証は困難である。

【０００７】

【発明が解決しようとする課題】本発明の目的は、ネットワーク上に存在する電子コンテンツの公開性を証拠付ける方策を提供することにある。

【０００８】本発明の他の目的は、ネットワーク上に存在する電子コンテンツの不改変性を証拠付ける方策を提供することにある。

【０００９】本発明のさらに他の目的は、電子コンテンツの公開性あるいは不改変性の証拠能力を高めることにある。

【００１０】

【課題を解決するための手段】本願の発明の概略を説明

すれば、以下の通りである。すなわち、本発明では、電子コンテンツの公開性の証明を希望する利用者に対して、予め登録された証人候補者の中から複数の証人または証明書生成器を選抜し、前記証人または証明書生成器に電子コンテンツの取得証明書を提供してもらうことで電子コンテンツの公開性の証明を実現する。なお、証人または証明書生成器は、登録された証人候補（証明書生成器を含む）のグループから無作為に選抜することができ、この場合には、無作為性を保証するために十分に大きな登録グループを用意することが好ましい。また、ここで証明書生成器にはたとえば証明書生成機能を備えたプロキシサーバを例示できる。

【００１１】本発明においては、証明書を発行するのは、利用者は勿論サービス機関とも関係のない証人または証明書生成器（第三者）である。このため利用者と利害関係がない証人により発行された証明書の証拠能力が高くなる。また、本発明はインターネットに代表されるコンピュータネットワークを利用して証明書を多数集めることができ、証人（証明書）の数を多くすることにより、証拠能力をさらに高めることができる。

【００１２】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。ただし、本発明は多くの異なる態様で実施することが可能であり、本実施の形態の記載内容に限定して解釈すべきではない。なお、実施の形態の全体を通して同じ要素には同じ番号を付するものとする。

【００１３】以下の実施の形態では、主に方法またはシステムについて説明するが、当業者であれば明らかなとおり、本発明は方法、システムの他、コンピュータで使用可能なプログラムコードが記録された媒体としても実施できる。したがって、本発明は、ハードウェアとしての実施形態、ソフトウェアとしての実施形態またはソフトウェアとハードウェアとの組合せの実施形態をとることができる。プログラムコードが記録された媒体としては、ハードディスク、ＣＤ－ＲＯＭ、光記憶装置または磁気記憶装置を含む任意のコンピュータ可読媒体を例示できる。

【００１４】本実施の形態で利用できるコンピュータシステムには、中央演算処理装置（ＣＰＵ）、主記憶装置（メインメモリ：ＲＡＭ(Random Access Memory)）、不揮発性記憶装置（ＲＯＭ(Read Only Memory)）等を有し、これらがバスで相互に接続される。バスには、その他コプロセッサ、画像アクセラレータ、キャッシュメモリ、入出力制御装置（Ｉ／Ｏ）等が接続される。バスには、適当なインターフェイスを介して外部記憶装置、データ入力デバイス、表示デバイス、通信制御装置等が接続されてもよい。その他、一般的にコンピュータシステムに備えられるハードウェア資源を備えることが可能なことは言うまでもない。外部記憶装置は代表的にはハードディスク装置が例示できるが、これに限られず、光磁気記憶装置、光記憶装置、フラッシュメモリ等半導体記憶装置も含まれる。なお、データの読み出しのみに利用でき得るＣＤ－ＲＯＭ等の読み出し専用記憶装置もデータあるいはプログラムの読み出しにのみ適用する場合には外部記憶装置に含まれる。データ入力デバイスには、キーボード等の入力装置、マウス等ポインティングデバイスを備えることができる。データ入力デバイスには音声入力装置も含む。表示装置としては、ＣＲＴ、液晶表示装置、プラズマ表示装置が例示できる。本実施の形態のコンピュータシステムには、パーソナルコンピュータ、ワークステーション、メインフレームコンピュータ等各種のコンピュータが含まれる。

【００１５】本実施の形態では、コンピュータシステム間の通信に主にインターネットを用いる例を説明するが、これに代えて複数のコンピュータシステムが相互に接続されるＬＡＮ、ＷＡＮ等を用いてもよい。これら接続に用いられる通信回線は、専用線、公衆回線の何れでも良い。また本発明は、単一のコンピュータシステムで実現されてもよい。

【００１６】各コンピュータシステムで利用されるプログラムは、他のコンピュータシステムに記録されていても良い。つまり、コンピュータシステムで利用する一部のプログラムをリモートコンピュータで分散的に処理または実行できる。なお、他のコンピュータシステムに記録されたプログラムをアドレスで参照する場合には、ＤＮＳ、ＵＲＬ等を用ることができる。

【００１７】本明細書においてインターネットという用語には、イントラネットおよびエクストラネットも含むものとする。インターネットへのアクセスという場合、イントラネットやエクストラネットへのアクセスをも意味する。コンピュータネットワークという用語には、公的にアクセス可能なコンピュータネットワークと私的なアクセスしか許可されないコンピュータネットワークとの両方が含まれるものとする。

【００１８】（実施の形態１）図１は、本発明の一実施の形態である証明システムの一例を説明する概念図である。本実施の形態のシステムには、サービス機関１０、利用者１１、証人または証明書生成器１２ａの集団である登録者グループ１２、コンテンツ発信機１３、電子コンテンツ１４を含む。サービス機関１０、利用者１１、証人または証明書生成器１２ａ、コンテンツ発信機１３は、たとえばインターネットに接続され、前記した一般的なコンピュータシステムが利用される。各コンピュータシステム間のデータの通信には、たとえばＨＴＴＰ（Hypertext Transfer Protocol)が用いられ、ＨＴＭＬ（Hypertext Markup Language）等の言語で記述されたデータを適当なブラウザを用いて表示できる。

【００１９】サービス機関１０は電子コンテンツの公開性または不改変性の証明を行う機関であり、詳細は後に

説明する。

【００２０】利用者１１は電子コンテンツの証明サービスを受けるものであり、前記したようなコンピュータシステムを利用してサービス機関１０にサービス要求（クライアント要求）を送信する。サービス要求に対して、サービス機関１０のコンピュータシステムはサーバとして機能し、たとえばＨＴＭＬ形式あるいはＸＭＬ（Extensible Markup Language)形式の文書を利用者１１のコンピュータシステムに返送し、利用者１１の表示画面に前記文書を表示する。

【００２１】証人または証明書生成器１２ａはサービス機関１０からの証明要求に応じて電子コンテンツの証明書を発行する者あるいはコンピュータシステムである。証人は証明書生成器１２ａであるコンピュータシステムを用いて自らの操作により証明書を発行する。証明書生成器１２ａは証人に操作されるほか、それ自体プロキシサーバとして動作するものを含む。プロシキサーバとして動作する場合には、自然人（証人）の操作は介在せず、証明書生成器１２ａにより自動的に証明書が発行される。 証明書生成器１２ａの詳細は後に説明する。

【００２２】コンテンツ発信機１３は、証明対象である電子コンテンツ１４が記録されているコンピュータシステムである。電子コンテンツ１４としては、たとえばホームページ等一般的なブラウザで表示される文書ファイルを例示できる。ただし、ブラウザで表示される文書ファイル（たとえばＨＴＭＬ文書、ＸＭＬ文書等）に限られず、ＦＴＰ(File Transfer Protocol)を用いたデータ転送が可能なデータファイル、パソコン通信の掲示板に掲示されたデータ、ネットニュースに投稿された文書等のデータであってもよい。なお、電子コンテンツ１４は、その記録形態が電子的なものであれば良く、たとえば紙媒体に記録されたものであっても、イメージリーダ等により電子データに変換されて記録される限り、電子コンテンツ１４に含まれる。

【００２３】図２は、実施の形態１のシステムのサービス機関および証明書生成器の一例を示したブロック図であり、図３は、証明要求受信部および証明作業管理部の一例を示したブロック図である。また、図４は、証明書作成管理部、証明書作成処理部および電子署名生成部の一例を示したブロック図である。

【００２４】サービス機関１０には、図２に示すように、証明要求受信部２１、証明書送信部２２、証明作業管理部２３、通信部２４、登録者選出部２５、登録者データベース２６、時計２７および電子コンテンツ取得部２８を備える。また、証明書生成器１２ａには、通信部２９、証明書作成管理部３０、電子コンテンツ取得部３１、時計３２、証明書作成処理部３３および電子署名生成部３４が備えられる。

【００２５】なお、前記各部あるいは以下説明する各部のさらに詳細な部分は、コンピュータシステムにプログラムとして与えられるソフトウェア機能として実現される。ソフトウェアはコンピュータシステムのハードウェア資源を利用してこれらの機能が実現される。

【００２６】証明要求受信部２１は、利用者１１からのサービス要求を受信する部分である。利用者１１からのサービス要求には、図３に示すように、たとえば利用者アドレス２１１、コンテンツアドレス２１２、証人条件２１３、証明機関２１４、証明精度２１５が含まれる。

【００２７】証明書送信部２２は、最終的に作成された証明書を利用者１１に送信する部分である。利用者１１とサービス機関１０とがインターネットで接続されている場合、証明書は、ＨＴＴＰに基づいてＨＴＭＬ文書等の形態で送信されるほか、ＦＴＰ、電子メール等で送信されてもよい。

【００２８】証明作業管理部２３は、サービス機関１０における証明作業を管理する部分である。図３に示すように、証明作業管理部２３には、たとえば利用者確認部２３１、利用者要求解析部２３２、利用履歴２３３、証明書発送部２３４、証明書受理部２３５、証人作業要請部２３６、時刻管理部２３７が含まれる。各部の機能は後にする方法の説明において詳述する。

【００２９】通信部２４は、証人のコンピュータシステムである証明書生成器１２ａまたはプロキシサーバとして機能する証明書生成器１２ａと通信するための制御機能を有する部分である。通信部２４を介して証明書生成器１２ａに証明要求が送信される。インターネットを介して通信する場合には、ＨＴＴＰに基づいてＨＴＭＬ文書等の形態で証明要求が送信されるほか、ＦＴＰ、電子メール等で送付されてもよい。

【００３０】登録者選出部２５は、利用者１１の要求を利用者要求解析部２３２で解析した結果、適当と判断される登録者を必要数だけ選抜する。選抜には登録者データベース２６を参照する。登録者として自然人を選抜するかプロキシサーバを選択するか、あるいは登録者を地域条件によって絞り込むか等がここで判断される。登録者が自然人である場合には年齢、性別、職業、等の条件で絞込みを行っても良い。なお、ここに挙げた条件はあくまでも例示であり、他の条件が付加されても良いことは勿論である。また、登録者データベース２６には、登録者の種類（自然人あるいはプロキシサーバ）、地域、年齢、性別、職業等前記条件のほか、証明履歴その他必要な情報が蓄積されていることは勿論である。登録者データベース２６はサービス機関１０の内部に記憶されている必要はなく、適当なＵＲＬ等のアドレスで特定される外部の記憶領域に記録されてもよい。

【００３１】時計２７は、システム内に備えられている時計である。時計２７はサービス機関１０の内部に備えられる必要はなく、外部の時計サービス機関の時計が参照されてもよい。

【００３２】電子コンテンツ取得部２８は、サービス要

求に含まれているコンテンツアドレスの電子コンテンツをサービス機関自ら取得するための取得部である。電子コンテンツ取得部２８は、記録されている電子コンテンツに適合したプロトコルに基づいてデータを取得できる機能を有する。たとえば、電子コンテンツがＨＴＭＬ文書であればＨＴＴＰを用いて電子データを取得できる。なお、ここで取得された電子コンテンツは、証人あるいはプロキシサーバにより取得された電子コンテンツとの同一性の判断に用いられる。

【００３３】通信部２９は、サービス機関１０のコンピュータシステムと通信するための制御機能を有する部分であり、通信部２４と同様な構成を有する。

【００３４】証明書作成管理部３０は、証人またはプロキシサーバの証明書生成器１２ａにおいて証明書の作成を管理する部分であり、図４に示すように、証明要求に含まれるコンテンツアドレスを参照して電子コンテンツ取得部３１を介し電子コンテンツ３０２を取得する。また、時計３２から時刻３０３を取得する。なお、電子コンテンツ取得部３１は電子コンテンツ取得部２８と同様な構成を有する。

【００３５】時計３２は証明書生成器１２ａのシステム内に備えられている時計である。時計３２は証明書生成器１２ａに備えられる必要はなく、外部の時計サービス機関の時計が参照されてもよい。

【００３６】証明書作成処理部３３は、証明書の作成処理を行う。証明書作成処理部３３では、証明要求に含まれているコンテンツアドレス２１２と、取得された電子コンテンツ３０２と、取得された時刻３０３とを１つの纏まったデータ３３１に生成し、この一纏まりのデータ３３１を電子署名生成部３４に引き渡す。

【００３７】電子署名生成部３４は、前記一纏まりのデータ３３１に電子署名を施す機能を持つ。電子署名生成部３４では、一纏まりのデータ３３１からハッシュ関数器３４１を通してハッシュコード３４２を生成する。さらに固有の秘密鍵暗号化手段３４３でハッシュコードを暗号化する。暗号化されたハッシュコード３４４には、公開鍵認証サーバ３６に登録されている公開鍵３４５が付されて証明書作成処理部３３に返送される。

【００３８】証明書作成処理部３３では、返送された暗号化ハッシュコード３４４と公開鍵３４５をデータ３３１（コンテンツアドレス２１２、電子コンテンツ３０２、時刻３０３を含む）に付加して証明書３３２を作成する。

【００３９】このように電子コンテンツ３０２のデータを含むデータ３３１をハッシュコード３４２に変換することにより、一般的に膨大なデータ量である電子コンテンツ３０２をデータ量の小さなハッシュコード３４２に変換して内容の同一性を判断しやすくすることができる。すなわちハッシュコードに変換すれば、変換前のデータがわずかに相違する場合でも、変換後のハッシュコードでは大きな変化として現れるので、複数の証明書を比較した場合に仮に電子コンテンツに改変が加えられていたときには、その改変がハッシュコードの大きな変化として現れる。

【００４０】なお、ここではハッシュコード３４２を用いているが、ハッシュコードに限らず、データを一義的に表すことができるその他のデータ変換法を用いても良い。また、図５に示すように、ハッシュコードを用いなくても良い。この場合、一纏まりのデータ３３１をすべて秘密鍵暗号化手段３４３で暗号化し、暗号化コンテンツアドレス３４６、暗号化電子コンテンツ３４７、暗号化時刻３４８に公開鍵３４５を付加して証明書３３２としても良い。

【００４１】次に、本発明の証明方法を説明する。本発明の証明方法の概要は、図１を用いて説明すれば以下の通りである。サービスの利用者１１はサービス機関１０に対してサービスを要求する（図中（１）のステップ）。この際、利用者１１は、サービス要求に際して証明対象の電子コンテンツを配信しているコンテンツ発信機のアドレスを送信し、必要であれば証人に関する諸条件を送信する。

【００４２】次に、サービス機関１０は、事前に登録されている証人または証明書生成器１２ａからなる登録者グループ１２の中から条件に適合する証人または証明書生成器１２ａを選出する（図中（２）のステップ）。この選出は無作為に行える。この際、サービス機関１０は選出された証人または証明書生成器１２ａに対して証明対象のアドレスを指定して、コンテンツの公開を証明するように要求する。

【００４３】次に、証人またはプロキシサーバ（証明書生成器１２ａ）はコンテンツ発信機１３に対してコンテンツを要求する（図中（３）のステップ）。

【００４４】次に、コンテンツが公開されていれば証明対象の電子コンテンツ１４が証人またはプロキシサーバ（証明書生成器１２ａ）に送信される（図中（４）のステップ）。

【００４５】次に、電子コンテンツ１４を閲覧した証人または証明書生成器１２ａはタイムスタンプを電子コンテンツ１４に添付し、電子署名などサービス機関１０の関知しない不可変処理を施してサービス機関１０に送信する（図中（５）のステップ）。これにより証明書の作成と返信が行われたこととなる。

【００４６】次に、証人または証明書生成器１２ａから受け取った証明書を単独でまたはひとつにまとめ、サービス機関１０が独自の不可変処理を施した後に利用者１１に転送する。証明書には証人の選出条件を添付できる。

【００４７】このように閲覧した電子コンテンツ１４に証人（またはプロキシサーバ）の不改変処理だけでなくサービス機関１０の不改変処理をも行うので、証明書の

改変は、利用者１１、第三者はもとよりサービス機関１０、証人（またはプロキシサーバ）１２ａにとってもきわめて困難である。これにより証明書の有効性を高めることができる。また、多数の証明書が集められ、コンテンツの内容の同一性が多数の証明書により証明された場合には、当該証明書によりコンテンツ内容の存在性（同一性）が立証できることとなる。なお、証明書の数が増すに従い、証拠能力が高まるものと考え得る。

【００４８】また、証明書を継続的に収集し、その内容が同一であることが証明されれば、当該期間の不改変性も証明されたことになる。

【００４９】以下フローチャートに従って、本発明の方法を詳細に説明する。図６は本発明の方法の全体フローを示したフローチャートである。

【００５０】本発明の方法は、利用者１１からのサービス要求によりサービスが開始する。まず、サービス機関１０のサーバが利用者１１からのサービス要求を受けると、サーバは利用者の確認を開始する（ステップ５００）。利用者の確認は証明作業管理部２３の利用者確認部２３１で行い、利用履歴２３３を参照する。利用者が正当な利用者であるか否かの判断を行い（ステップ５０１）、正当利用者である場合には次ステップ５０２に進み、正当利用者でない場合はエラー処理を行って終了する（ステップ５０３）。

【００５１】次に、利用者のサービス要求の内容を解析する（ステップ５０２）。サービス要求の解析は証明作業管理部２３の利用者要求解析部２３２で行う。解析の結果、利用者の要求が妥当（サービス可能）であるか否かの判断を行い（ステップ５０４）、妥当であれば次ステップ５０５に進み、妥当でない場合にはエラー処理を行って終了する（ステップ５０６）。

【００５２】次に、登録者の選出を行う（ステップ５０５）。登録者の選出は登録者選出部２５で行う。選出者がいるか否かの判断を行い（ステップ５０７）、選出者がいる場合には次ステップ５０８に進み、いない場合にはエラー処理を行って終了する（ステップ５０９）。

【００５３】次に、証明作業を行う（ステップ５０８）。証明作業は、証人作業要請部２３６からの証明要求の発送と、証明要求を受けた証人側に作業からなる。

【００５４】次に証人側から証明書の作成されるか否かの判断を行う（ステップ５１０）。証明書が作成された場合には、次ステップの証明書受理作業（ステップ５１１）に進み、証明書が作成されない場合には、新たな登録者を選出するためにステップ５０５に戻る。

【００５５】送付された証明書は証明書受理作業に付される（ステップ５１１）。その後証明書が受理されるか否かの判断を行い（ステップ５１２）、証明書が受理された場合には次ステップの証明書発送作業（ステップ５１３）に進み、証明書が受理されない場合には新たな登録者を選出するためにステップ５０５に戻る。

【００５６】次に証明書発送作業に進み（ステップ５１３）、その後証明期間が終了したか否かの判断を行う（ステップ５１４）。証明期間が終了していない場合にはタイマー５１５を参照して新たな証明時刻に登録者選出（ステップ５０５）に戻り、前記証明作業を繰り返す。証明期間が終了している場合には、サービスを終了する（ステップ５１６）。

【００５７】以下、さらに詳細に、前記各ステップの詳細を説明する。図７は、利用者がサービス要求をする場合の利用申請ダイアログの一例を示す表示図である。

【００５８】利用者１１がサービス機関１０にサービス要求を出す場合には、ダイアログ８００に必要事項を記入して送信することにより行える。記入事項としては、たとえば証明対象の電子コンテンツ１４が記録されているアドレスを入力フィールド８０１に記入する。アドレスはたとえばＵＲＬで記入する。本実施の形態では「http://www.ibm.com」が指定されている。また、利用者１１のプロファイルとして、利用者アドレスを入力フィールド８０２に記入する。ここでは「test@trl.ibm.com」の電子メールアドレスが記入されている。また、証明条件として、期間、精度、必要証明数、証人の国籍、年齢、職業、証明履歴を各々入力フィールド８０３～８０９に入力する。なお、ここで示した証明条件はあくまでも例示でありこのすべてを必要とするものではない。また、その他の証明条件を付加することもできる。

【００５９】入力が終了すれば、「ＯＫ」ボタン８１０を押してデータを送信する。送信をキャンセルする場合には「Cancel」ボタン８１１を押してキャンセルする。

【００６０】なお、ここでは利用者１１のコンピュータシステムにインストールされたアプリケーションプログラムの一部の機能として実現されるような入力ダイアログ８００を例示したが、たとえば適当なブラウザに入力画面用の表示文書を表示させてもよい。

【００６１】「ＯＫ」ボタン８１０を押すことにより、各入力フィールドに入力されたデータはサービス機関１０のサーバに送信される。データを受け取ったサービス機関のサーバは利用者確認を開始する（ステップ５００）。図８は、利用者確認ステップの詳細を示したフローチャートである。

【００６２】まずサービス要求（入力データ）に含まれる利用者のアドレス（返信アドレス）を確認する（ステップ５１７）。返信アドレスに確認メールを送信し、当該アドレスに確認メールが到達可能か否かを判断する（ステップ５１８）。メール到達が可能であれば次ステップ５１９に進み、メール到達が不可能であれがエラー処理を行って処理を終了する（ステップ５２０）。

【００６３】次に、利用者の利用履歴を確認する（ステップ５１９）。利用履歴確認は、利用履歴ファイル２３３を参照して、当該利用者１１の過去の利用が妥当か否かで判断する（ステップ５２１）。過去の利用が妥当で

ない場合、たとえば過去に料金の不納等がある場合には利用履歴ファイル２３３にその旨のデータが利用者ごとに蓄積されており、このデータに基づいて今回利用の妥当性を判断する。過去の利用が不当の場合には、エラー処理を行い（ステップ５２３）、過去に不当な利用がない場合には今回の利用を許可することとして次ステップ５２２に進む。なおエラー処理には利用できない旨のメッセージ送信を含むことができる。

【００６４】次に、手数料の支払い方法の確認を行う（ステップ５２４）。支払い方法はクレジットカードによる決済、電子マネー、チケットによる決済等ネットワーク上で利用できる決済サービスのほか、利用者ごとの決済口座等を設けて口座残高管理により行う等任意の決済方法を採ることができる。その後、支払い能力が信頼できるか否かの判断を行い（ステップ５２４）、信頼に足る場合には利用者確認を終了して次ステップに進む（ステップ５２５）。支払い能力が信頼に足りない場合はエラー処理を行って終了する（ステップ５２６）。

【００６５】図９は利用者要求を解析するステップ（ステップ５０２）の詳細を示したフローチャートである。利用者１１からのサービス要求（入力データ）に含まれる時刻精度に着目し（ステップ５２７）、要求時刻精度としてストアする（ステップ５２８）。同様に入力された証明期間を要求証明機関として、証人数を要求証人数として、証人条件を要求証人条件として、証明コンテンツアドレスを要求証明コンテンツアドレスとしてストアする（ステップ５２９～５３６）。なお、その他の要求事項がある場合には適宜要求項目として同様にストアできることは勿論である。また、各要求事項（要求データ）をストアする際に、要求が妥当か否かの判断をすることができる。たとえば時刻精度が実現不可能な程度に高い場合（たとえば０．０１秒等）、証明機関が実現不可能な程度に長い場合（たとえば１００年等）、証人数が登録者グループの総数を超えるような場合には不当な要求に該当する。不当な要求の場合にはエラー処理により処理を終了できる。また、証人の種類として、自然人であるかプロキシサーバであるかを選択することもできる。

【００６６】利用者の要求がサービス可能な範囲にある場合には、要求証明コンテンツアドレスの確認を行う（ステップ５３７）。これはサービス機関自らが証明対象の電子コンテンツの存在確認を行うものであり、コンテンツの取得を試みて取得可能であるか否かの判断を行うことにより判断する（ステップ５３８）。コンテンツの取得に成功すればコンテンツの存在が推認され、利用者要求の解析ステップを終了する（ステップ５３９）。取得に失敗した場合にはその後の証人作業を進めても無駄になる可能性が極めて大きいのでエラー処理を行い、処理を終了する（ステップ５４０）。

【００６７】図１０は、登録者選出のステップ（ステップ５０５）の詳細を示したフローチャートである。登録者の選出は、登録者データベース２６を参照して行う。登録者データベース２６には、登録者の地域、年齢、性別、職業、さらに証明履歴等がデータベース化されて記録されている。本ステップでは、これら登録者のデータベースにより、利用者の要求に従った登録者を選別する。すなわち利用者要求の地域、年齢等の条件により、地域条件の絞込み（ステップ５４１）、年齢条件の絞込み（ステップ５４２）、性別条件の絞込み（ステップ５４３）、職業条件の絞込み（ステップ５４４）、証明履歴条件の絞込み（ステップ５４５）を行う。なお、これら条件に絞り込む順番は任意であり、またすべての条件を適用する必要はない。逆にその他の絞込み条件を付加しても良い。

【００６８】次に、証人（登録者）の条件に適合する選出者がいるか否か（必要な数の選出者が選抜されたか否か）を判断する（ステップ５４６）。必要登録者の選出ができた場合には、次ステップ５４７に進み、選出できなかった場合にはエラー処理を行って終了する（ステップ５４９）。登録者が選出された場合には、その中からさらに乱数を用いて無作為に登録者を選出し（ステップ５４７）、登録者の選出を終了する（ステップ５４８）。このように所定の条件で絞り込むことにより利用者の要求を満足しつつ、要求の範囲内で無作為に登録者を選抜することにより、証人選抜の恣意を排除して公平性を担保できる。なお、前記絞り込みの条件は必須のものではなく、また、他の絞込み条件を付加しても良い。また、登録者の選抜は無作為に行う必要はなく、たとえば登録者のシステム条件等で順位付けしてこの順位の順番で選抜しても良い。あるいは選抜回数を均一化するために既選抜回数の少ない順に選抜してもよい。

【００６９】図１１は、証明作業の詳細を示したフローチャートである。まず、サービス機関１０から証人に対して証人作業の要請を行う（ステップ５５０）。要請は、前記した登録者選出作業で選出された証人（または証人機能を自動的に実現するプロキシサーバ）に対して行う。また要請は図１２に示すようなダイアログ８２０を証人の表示画面に表示して行うことができる。図１２は、証人作業を行う意思確認のダイアログの一例を示した表示図である。ダイアログ８２０には証人に対する証明書作成を要請する旨のメッセージとともに、「OK」ボタン８２１、「Cancel」ボタン８２２を表示する。証人は要請を受け入れる場合には「OK」ボタン８２１を押すことにより意思表示する。要請を受け入れない場合には「Cancel」ボタン８２２を押すこととなる。

【００７０】前記「OK」または「Cancel」により、証人が証人作業を受け入れたか否かをサービス機関１０は判断し（ステップ５５１）、受け入れた場合には次ステップ５５２に進み、受け入れない場合にはエラー処理を行って処理を終了する（ステップ５５３）。

15

【００７１】なお、証人側のシステムがプロキシサーバである場合には、所定のプログラムにより証人作業を行うか否かを判断して、自動的に「OK」または「Cancel」データをサービス機関のサーバに返送することができる。

【００７２】次にサービス機関１０のシステムは時計同期をとる（ステップ５５２）。時計同期は、サービス機関のシステムと証人側のシステムの時計を合わせるためのものであり、標準となる外部時計を参照して行う。外部時計のサービスとしてたとえば「www.eecis.udel.edu/~ntp/」を例示できる。図１３は、時計同期の際に用いられる外部時計のシステムを表すブロック図（図１３（ａ））と時計同期の方法を示すフローチャート（図１３（ｂ））である。まず、サービス機関のシステムは利用する時計サービスの選出を行い（ステップ５５８）、当該時計サービスの利用を試みてサービスが利用できるか否かを判断し（ステップ５５９）、サービスが利用できなければ他の時計サービスの利用を試み（ステップ５６１）、サービスが利用できた場合には証人側に時計サービスのアドレスを送信する（ステップ５６０）。証人側では、当該アドレスの時計サービスを利用して自己の時計あわせを行い（ステップ５６２）、サービスが利用できたか否かを判断した上で（ステップ５６３）、サービス利用できた場合にはサービス機関に正常終了した旨の返信を行い（ステップ５６４）、サービスが利用できない場合にはエラーした旨の返信をサービス機関に返す（ステップ５６６）。この場合他の時計サービスの利用を試みることができる。

【００７３】なお、ここでは外部の時計サービスを利用して時計同期を行う方法を説明したが、内部時計を用いて同期を図っても良い。図１４は、内部時計を利用して時刻同期を図るシステムを表すブロック図（図１４（ａ））と、方法を示すフローチャート（図１４（ｂ））である。サービス機関１０と証人１２ａの各々のシステムに時刻同期処理部２３ａ、３０ａを備える。まず、サービス機関の時計２７から時刻を取得し（ステップ５６７）、平均パケット伝送時間を計測する（ステップ５６８）。その後サービス機関から証人に時刻を送出し（ステップ５６９）、証人側のシステムはサービス機関からの時刻を受信する（ステップ５７０）。証人側のシステムでは、内部時計３２と受信したサービス機関からの時刻および平均パケット伝送時間を勘案して証人側の時刻を修正する（ステップ５７１）。この場合、証人の時刻は修正された時刻を用いることになる。

【００７４】このようにして時計の同期を図った後、図１１に示す通り、サービス機関から証人に証明条件の送信を行う（ステップ５５４）。証明条件には電子コンテンツのアドレスが含まれる。また、証明条件には証明書の作成様式、たとえばハッシュ関数を用いてハッシュコードを生成するか等の情報を含めることができる。

16

【００７５】次に、証人は証明書の作成を行う（ステップ５５５）。図１５は証明書作成のステップを詳細に示したフローチャートである。

【００７６】まず、証人は、証明条件送信のステップ（ステップ５５４）で送付されたコンテンツアドレスにアクセスし、電子コンテンツ１４の取得を試みる（ステップ５７２）。電子コンテンツ１４が取得できたか否かを判断し（ステップ５７３）、取得できた場合には次ステップ５７６に進む。取得できなかったときには再試行を行い（ステップ５７４）、再度ステップ５７２に戻る。再試行回数が所定の回数に達した場合には電子コンテンツの取得が失敗したと判断しエラー処理を行って処理を終了する（ステップ５７５）。

【００７７】電子コンテンツの取得の後、時刻の取得を試みる（ステップ５７６）。 時刻が取得できたか否かを判断し（ステップ５７７）、取得できた場合には次ステップ５８０に進む。取得できなかったときには再試行を行い（ステップ５７８）、再度ステップ５７６に戻る。再試行回数が所定の回数に達した場合には時刻の取得が失敗したと判断しエラー処理を行って処理を終了する（ステップ５７９）。

【００７８】次に、取得された電子コンテンツと時刻をコンテンツアドレスとともに一纏まりのデータ３３１にまとめる（ステップ５８０）。その後電子署名を施して（ステップ５８１）、証明書の作成ステップを終了する。

【００７９】図１６は、電子署名を施す前段階の証明書作成ダイアログを示す表示画面図である。ダイアログ８３０には、電子コンテンツのアドレスがフィールド８３１に表示され、証明対象である電子コンテンツ１４が表示フィールド８３２に表示されている。また、当該アドレスにアクセスした結果の表示すなわちコンテンツに対して証明を与えるかどうかを問うメッセージとともに、「OK」ボタン８３４、「Cancel」ボタン８３５を表示し、証明書発行の確認を促す。ここで証人が「OK」ボタン８３４を押せば電子署名が施されて証明書が発行されることとなる。

【００８０】図１７は、電子署名のステップを詳細に示したフローチャートである。ステップ５８０でコンテンツアドレス、電子コンテンツおよび時刻からなるデータを生成した後、このデータのハッシュコードを生成する（ステップ５８２）。ハッシュコードに変換することにより証明書間の同一性をハッシュコードを参照して判断することが可能になり、判断を容易にできる。なお、前記システムの説明部分で述べた通り、必ずしもハッシュコードに変換する必要はない。また、データが一義的に変換される要件を満たせば、ハッシュ関数以外の関数を用いてもよい。ハッシュに変換しない場合、その他の関数を用いてコード変換を行う場合は、コンテンツアドレス、電子コンテンツおよび時刻からなるデータあるいは

その変換コードが次ステップで暗号化されることは言うまでもない。

【００８１】その後ハッシュコードを秘密鍵で暗号化する（ステップ５８３）。証人しか知りえない秘密鍵を用いてハッシュコードを暗号化することにより、証明書の改変が証人以外には実質的に不可能になる。なお、後に説明するように証明書はサービス機関によってさらに秘密鍵で暗号化される。２重に暗号化されるため、利用者に提供される段階での証明書は証人あるいはサービス機関であっても改変は不可能である。この結果、証明書の不改変に対する信頼性を高めることができる。

【００８２】次に、秘密鍵で暗号化されたハッシュコードに電子コンテンツ、コンテンツアドレスおよび時刻を添付して（ステップ５８４）電子署名を終了する。このようにして証人作業段階での証明書が生成される。なお、証明書には公開鍵登録サービス機関の公開鍵を添付できる。これにより証明書の通信を暗号化して安全に通信できる。

【００８３】上記の通り作成された証明書は、図１１に示すようにサービス機関の証明作業管理部２３に返信される（ステップ５５６）。このようにして証明作業が終了する。

【００８４】図１８は証明書受理作業のステップを詳細に示したフローチャートである。サービス機関のサーバは、証人から返信された証明書を受け取ると、証明作業の依頼時刻と証明書に添付された時刻と現在時刻とを比較し（ステップ５８５）、時刻差が利用者の要求を満たしているか否かを判断する（ステップ５８６）。要求が満たされているときには次ステップ５８７に進み、要求が満たされていないときにはエラー処理を行って処理を終了する（ステップ５８８）。

【００８５】次に、証明書に添付された電子コンテンツの内容とサービス機関が先に取得した電子コンテンツの内容とを比較する（ステップ５８７）。証明書のコンテンツと取得したコンテンツの内容が一致しているか否かを判断し（ステップ５８９）、一致している場合には次ステップ５９０に進み、一致しない場合にはエラー処理を行って終了する（ステップ５９１）。なお、コンテンツの同一性の判断にはハッシュコードを用いることができる。また、証明書が複数存在する場合にはサービス機関が先に取得したコンテンツに代えて複数証明書同士を比較することができる。

【００８６】次に、証明書の証人署名を確認する（ステップ５９０）。証人署名が正しいか否かを判断し（ステップ５９２）、署名が正しいときにはサービス機関の電子署名を加えて（ステップ５９３）、証明書の受理ステップを終了する。証明書の電子署名が正しくない場合にはエラー処理をして終了する（ステップ５９４）。

【００８７】このように証人の署名に加えてサービス機関が署名を加えることにより、第三者、利用者は勿論、サービス機関、証人ともに証明書に改変を加えることは不可能になる。これにより証明書の信頼性を高く保つことができ、証明書の証拠の成立性を高くすることができる。

【００８８】なお、電子署名には、たとえば「www.moj.go.jp/PUBLIC/MINJI02/pub_minji02_04.htm」で提供されているサービスを例示できるがこれに限られず、署名物の不改変性を担保できるものであればどのような電子署名であっても良い。

【００８９】図１９はサービス機関により作成された最終的な証明書の一例を示した表示画面図である。フレーム８４０内のフィールド８４１にコンテンツの発行者、証明日等書誌的事項が表示され、電子コンテンツがフィールド８４２に表示されている。さらに証人およびサービス機関によるハッシュコードがフィールド８４３に表示されている。

【００９０】なお、図２０に示すように、複数のコンテンツを１つの証明書内に表示することもできる。図２０には、フレーム８５０内のフィールド８５１にコンテンツの発行者、証明日等書誌的事項が表示され、複数の電子コンテンツがフィールド８５２～８５５に表示されている。さらに証人およびサービス機関によるハッシュコードがフィールド８５６に表示されている。

【００９１】図２１は証明書発送作業のステップを詳細に示したフローチャートである。サービス機関１０が利用者１１に証明書を発送するに際して、公証人サービスを利用するか否かの判断をする（ステップ５９５）。公証人サービスを利用する場合には公証人サービス（ステップ５９６）を利用した後に次ステップ５９７に進み、サービスを利用しない場合にはステップ５９６をパスしてステップ５９７に進む。次に証明書蓄積サービスを利用するか否かを判断し（ステップ５９７）、サービスを利用する場合には証明書蓄積サービス（ステップ５９８）を利用した後に次ステップ５９９に進み、サービスを利用しない場合にはステップ５９８をパスしてステップ５９９に進む。最後に利用者１１に証明書を発送する（ステップ５９９）。

【００９２】このようにして本発明の証明方法を終了する。このような方法により、前記したシステムを用いて電子コンテンツの存在証明を収集することができる。これにより電子コンテンツの存在は勿論、継続的に同一の電子コンテンツが存在していたこと、つまり電子コンテンツの不改変性を証明できる。また、証人あるいはプロキシサーバは、利用者にとっては無関係の第三者であり、電子コンテンツが厳密な意味でも公開されていたことが立証できる。つまり、既存の証明機関による証明であっても、証明機関に対して公開されているとはいえ、公衆に公開されているとは厳密には言えない。しかし本発明の証人あるいはプロキシサーバは不特定の第三者であり公衆とみなせる存在である。よって公衆たる証人等

に公開されていることから電子コンテンツが厳密な意味でも公開されていたこと（公衆性）が証明できたことになる。

【００９３】なお、証明期間が長期に渡る場合には、特定の期日を中心に前記証明書または複数の証明書群によって電子コンテンツの同一性が証明されるほか、特定の期日を境に電子コンテンツが改変されたことも立証しうる。つまり、継続的に証明書を収集し、ある期日を境に証明書に添付される電子コンテンツまたはそのハッシュコードが変化しているときには、その期日をもって電子コンテンツが改変されたことを立証できる。言い換えれば、その期日の前の不改変性と、改変の期日と、その期日後の不改変性を証明できる。さらに改変が複数回に渡るときには、改変の期日および同一性が保たれている期間を立証できる。

【００９４】なお、証人の登録は以下のようにして行える。図２２は証人登録のシステムを示すブロック図（図２２（ａ））およびその方法を示すフローチャート（図２２（ｂ））である。証人登録はサービス機関１０と証明書生成器１２ａとを用いて行える。サービス機関１０のサーバには登録者データベース４０、証人登録管理部４１、通信部４２を備え、証明書生成器１２ａには通信部４３、証人登録部４４を備える。まず、証明書生成器１２ａから通信部４３、４２を介して証人の登録申請をサービス機関に発し、サービス機関はこれを受理する（ステップ６００）。サービス機関は証人登録管理部４１でこれを審査し（ステップ６０１）、登録者要件を満たすか否かを判断する（ステップ６０２）。要件を満たす場合には登録者データベース４０に登録して終了し（ステップ６０３）、要件を満たさない場合にはエラー処理をして終了する（ステップ６０４）。

【００９５】（実施の形態２）図２３は、本発明の他の実施の形態である証明システムの一例を示した概念図である。本実施の形態のサービス機関１０、利用者１１、登録者グループ１２、証人または証明書生成器１２ａ、コンテンツ発信機１３、証明対象の電子コンテンツ１４は実施の形態１と同様である。本実施の形態では、電子公証サービス機関９００を利用する。電子公証サービス機関９００は、たとえば「www.surety.com」で提供されているような公証人サービスをいい、実施の形態１の電子署名に代えて、公証人の信用性を利用して証明書の証明価値を担保するものである。以下実施の形態２の説明において実施の形態１と同様な場合には説明を省略する。

【００９６】図２４は、実施の形態２のシステムのサービス機関および証明書生成器の一例を示したブロック図であり、図２５は、証明書作成管理部および証明書作成処理部の一例を示したブロック図である。本実施の形態のサービス機関１０（証明要求受信部２１、証明書送信部２２、証明作業管理部２３、通信部２４、登録者選出部２５、登録者データベース２６、時計２７および電子コンテンツ取得部２８）は、実施の形態１と同様であり、証明書生成器１２ａには、実施の形態１と同様な通信部２９、証明書作成管理部３０、電子コンテンツ取得部３１、時計３２および証明書作成処理部３３を備える。

【００９７】本実施の形態２では、証明サービスの方法およびシステムにおいて公証人サービス機関９００を構成要件として含む。実施の形態１で説明したように証明作業管理部２３および証明書作成処理部３３では、各々サービス機関１０および証明書生成器１２ａにおける電子署名を行ったが、本実施の形態では、電子署名に代えて公証人サービス機関９００の公証を用いる。このため本実施の形態のシステムでは実施の形態１の電子署名生成部３４を含まない。

【００９８】図２５に示すように、証明書作成管理部３０では、実施の形態１で説明したコンテンツアドレス２１２、電子コンテンツ３０２、時刻３０３に加えて証人プロファイル９０１を用意する。

【００９９】証明書作成処理部３３では、これらコンテンツアドレス２１２、電子コンテンツ３０２、時刻３０３および証人プロファイル９０１からデータ９０２を生成し、このデータ９０２を電子公証サービス機関９００に送付して、認証申請を行う。認証されたデータは証明書９０３として証明書作成処理部３３が電子公証サービス機関９００から受け取る。認証済みの証明書９０３が証明書としてサービス機関１０に転送される。

【０１００】本実施の形態によれば、証人あるいはサービス機関の電子署名がなくても、公証サービス機関による認証により証明書の不改変性が担保できる。勿論証明書９０３の改変は利用者あるいは第三者にも不可能であり、証明書９０３の証拠としての能力が有効に担保できる。

【０１０１】以上、本発明者によってなされた発明を発明の実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能である。

【０１０２】たとえば、図２６に示すように、利用者１１とコンテンツ発信機１３（電子コンテンツ１４）が同一のコンピュータシステム内に存在しても良い。

【０１０３】また、図２７に示すように、サービス機関１０が自ら有する電子コンテンツ１４の証明に用いても良い。この場合、利用者とサービス機関とが同一のコンピュータシステムで構成されることるため、実施の形態１で説明したようなサービス機関による電子署名で証明書の改変を防止する手段は好ましくない。証明書の改変性を皆無にする、つまり証明書の証拠価値を高くするためには公証サービス機関による認証を受けることが好ましい。

【０１０４】また、実施の形態１では、サービス機関と

証人との２重の電子署名により、実施の形態２では公証機関の認証により証明書の不改変性を担保したが、サービス機関、利用者、証人以外の第三者と、証人またはサービス機関との２重の電子署名を適用しても良い。さらに、これら２重の電子署名に加えて公証サービスを受けても良い。

【０１０５】まとめとして、本発明の構成に関して以下の事項を開示する。

（１）コンピュータシステムまたはコンピュータネットワークを利用した電子コンテンツを証明する方法であって、（ａ）前記証明のサービス機関が、証人または証明書生成器に対し、証明書作成要求を送信するステップと、（ｂ）前記証人または証明書生成器が、前記サービス機関の証明書作成要求に応じて、前記電子コンテンツを取得するステップと、（ｃ）証明書を作成するステップと、を含む電子コンテンツの証明方法。

（２）前記証明書には、前記電子コンテンツまたは前記電子コンテンツを一義的に表すデータを含む前記（１）記載の証明方法。

（３）前記証明方法には、さらに、（ｄ）前記証明書が、前記サービス機関に蓄積されるステップまたは前記利用者に送付されるステップを含む前記（１）または（２）記載の証明方法。

（４）前記証明書には、前記電子コンテンツのアドレス情報および前記証明の時刻情報を含む前記（１）～（３）の何れか一項に記載の証明方法。

（５）前記証明書の作成ステップには、前記証明書に署名するステップを含む前記（１）～（４）の何れか一項に記載の証明方法。

（６）前記署名ステップには、前記証人または証明書生成器による第１の署名ステップと、前記サービス機関による第２の署名ステップとを含む第１の構成、または、公証人サービス機関による署名ステップを含む第２の構成、の何れかの構成を有する前記（５）に記載の証明方法。

（７）前記署名には、公開鍵暗号方式による暗号化を用い、署名者以外の改変を不可能とした前記（５）、（６）記載の署名方法。

（８）前記署名には、前記証人、証明書生成器またはサービス機関の秘密鍵が各々用いられる前記（５）～（７）の何れか一項に記載の証明方法。

（９）前記電子コンテンツを一義的に表すデータが、ハッシュコードである前記（２）～（８）の何れか一項に記載の証明方法。

（１０）前記証明書の伝送には、公開鍵認証サービス機関の公開鍵が付される前記（１）～（９）の何れか一項に記載の証明方法。

（１１）前記利用者のサービス要求には、前記電子コンテンツのアドレス情報が含まれ、さらに前記証人の属性に関する要求情報および前記証明に関する要求情報が含まれる前記（１）～（１０）の何れか一項に記載の証明方法。

（１２）前記証明書作成要求は、前記利用者の要求に応じて、単一もしくは複数の期日に、または、単一もしくは複数の期間を定めて継続的に、前記証人または証明書生成器に送信される前記（１）～（１１）の何れか一項に記載の証明方法。

（１３）前記証人または証明書生成器は、無作為に選出される第１の構成、前記利用者の要求を満足する証人または証明書生成器の集合から選出される第２の構成、または、前記利用者の要求を満足する証人または証明書生成器の集合から無作為に選出される第３の構成、の何れかの構成を有する前記（１）～（１２）の何れか一項に記載の証明方法。

（１４）前記サービス機関と前記証人または証明書生成器との間の時刻は、同期がとられる前記（１）～（１３）の何れか一項に記載の証明方法。

（１５）前記時刻の同期は、外部時計サービスを用いる方法、または、前記サービス機関および証人または証明書生成器の各々の内部時計を平均パケット伝送時間を用いて補正する方法、の何れかの方法で行う前記（１４）記載の証明方法。

（１６）コンピュータシステムまたはコンピュータネットワークを利用した電子コンテンツを証明するシステムであって、証人または証明書生成装置に対し証明書作成要求を送信する手段と、前記証明書作成要求に応じて前記電子コンテンツを取得する手段と、証明書を作成する手段と、を備えた電子コンテンツの証明システム。

（１７）前記証明書には、前記電子コンテンツまたは前記電子コンテンツを一義的に表すデータを含む前記（１６）記載の証明システム。

（１８）前記証明システムには、さらに、　前記証明書を、前記サービス機関のコンピュータシステムに蓄積する手段または前記利用者に送付する手段の何れかを備えた前記（１６）または（１７）記載の証明システム。

（１９）前記証明書には、前記電子コンテンツのアドレス情報および前記証明の時刻情報が含まれる前記（１６）～（１８）の何れか一項に記載の証明システム。

（２０）前記証明書の作成手段には、前記証明書に署名する手段を含む前記（１６）～（１９）の何れか一項に記載の証明システム。

（２１）前記署名手段には、前記証人または証明書生成器による第１の署名手段と、前記サービス機関による第２の署名手段とを含む第１の構成、または、公証人サービス機関による署名手段を含む第２の構成、の何れかの構成を有する前記（２０）記載の証明システム。

（２２）　前記署名手段には公開鍵暗号方式による暗号化手段を用い、署名者以外の改変を不可能とした前記（２０）、（２１）記載の署名システム。

（２３）前記署名手段には、前記証人、証明書生成器ま

たはサービス機関の秘密鍵が各々用いられる前記（１６）～（２２）の何れか一項に記載の証明システム。

（２４）コンピュータシステムまたはコンピュータネットワークを利用した電子コンテンツの公開性または不改変性を証明するサービス機関のシステムであって、利用者のサービス要求を受理し、前記サービス要求を解析する手段と、証人または証明書生成器が登録された登録者グループから、前記証人または証明書生成器を選出する手段と、前記証人または証明書生成器に証明書作成要求を送信する手段と、前記証人または証明書生成器から返送された証明書を受理する手段と、前記証明書を前記利用者に送信する手段と、を備えた前記サービス機関の証明システム。

（２５）前記証明書の受理手段には、前記証明書に電子署名を施す手段が含まれる前記（２４）記載のシステム。

（２６）前記電子署名は、前記サービス機関の秘密鍵を用いて前記証明書を暗号化する手段である前記（２５）記載のシステム。

（２７）前記サービス要求には、前記証人に関する条件が含まれ、前記証人または証明書生成器を選出する手段には、前記証人に関する条件を満足する証人群を選出する手段を含む第１の構成、前記証人または証明書生成器を選出する手段には、無作為に前記証人または証明書生成器を選出する手段を含む第２の構成、の何れかの構成を有する前記（２４）～（２６）の何れか一項に記載のシステム。

（２８）前記サービス要求には、前記証明の期日または期間情報が含まれ、前記証明書作成要求を送信する手段には、前記証明書作成要求が前記期日または前記期間内において継続的に送信される手段を含む前記（２４）～（２７）の何れか一項に記載のシステム。

（２９）コンピュータシステムまたはコンピュータネットワークを利用した電子コンテンツの公開性または不改変性を証明する証人または証明書生成器のシステムであって、サービス機関からの証明書作成要求を受理する手段と、前記証明書作成要求に含まれる前記電子コンテンツのアドレスにアクセスし、前記電子コンテンツを取得する手段と、前記電子コンテンツまたは前記電子コンテンツを一義的に表すコードを含む証明書を作成する手段と、前記証明書を前記サービス機関に返信する手段と、を備えた前記証人または証明書生成器のシステム。

（３０）前記証明書の作成手段には、前記証明書に電子署名を施す手段が含まれる前記（２９）記載のシステム。

（３１）前記電子署名は、前記証人または証明書生成器の秘密鍵を用いて前記証明書を暗号化する手段である前記（３０）記載のシステム。

（３２）前記電子コンテンツを一義的に表すコードは、ハッシュコードである前記（２９）～（３１）の何れか一項に記載のシステム。

（３３）前記証明書の作成手段には、前記サービス機関の時計と同期がとられている時刻情報を付加する手段を含む前記（２９）～（３２）の何れか一項に記載のシステム。

（３４）コンピュータシステムまたはコンピュータネットワークを利用した電子コンテンツの公開性または不改変性を証明するプログラムコードが記録された媒体であって、前記プログラムコードには、利用者または自己のサービス要求に応じて、証人または証明書生成装置に対し、証明書作成要求を送信するプログラムコードと、前記サービス機関の証明書作成要求に応じて、前記電子コンテンツを取得するプログラムコードと、前記電子コンテンツまたは前記電子コンテンツを一義的に表すデータを含む証明書を作成するプログラムコードと、前記証明書を、前記サービス機関のコンピュータシステムに蓄積するプログラムコードまたは前記利用者に送付するプログラムコードの何れかと、を含むプログラムコードが記録された媒体。

（３５）コンピュータシステムまたはコンピュータネットワークを利用した電子コンテンツの公開性または不改変性を証明するプログラムコードが記録された媒体であって、前記プログラムコードには、利用者のサービス要求を受理し、前記サービス要求を解析するプログラムコードと、証人または証明書生成器が登録された登録者グループから、前記証人または証明書生成器を選出するプログラムコードと、前記証人または証明書生成器に証明書作成要求を送信するプログラムコードと、前記証人または証明書生成器から返送された証明書を受理するプログラムコードと、前記証明書を前記利用者に送信するプログラムコードと、を含むプログラムコードが記録された媒体。

（３６）コンピュータシステムまたはコンピュータネットワークを利用した電子コンテンツの公開性または不改変性を証明するプログラムコードが記録された媒体であって、前記プログラムコードには、サービス機関からの証明書作成要求を受理するプログラムコードと、前記証明書作成要求に含まれる前記電子コンテンツのアドレスにアクセスし、前記電子コンテンツを取得するプログラムコードと、前記電子コンテンツまたは前記電子コンテンツを一義的に表すコードを含む証明書を作成するプログラムコードと、前記証明書を前記サービスに返信するプログラムコードと、を含むプログラムコードが記録された媒体。

【０１０６】

【発明の効果】本願で開示される発明のうち、代表的なものによって得られる効果は、以下の通りである。

【０１０７】すなわち、ネットワーク上に存在する電子コンテンツの公開性を証拠付ける方策を提供できる。また、ネットワーク上に存在する電子コンテンツの不改変

性を証拠付ける方策を提供できる。さらに、電子コンテンツの公開性あるいは不改変性の証拠能力を高めることができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態（実施の形態１）である証明システムの一例を説明する概念図である。

【図２】実施の形態１のシステムのサービス機関および証明書生成器の一例を示したブロック図である。

【図３】証明要求受信部および証明作業管理部の一例を示したブロック図である。

【図４】証明書作成管理部、証明書作成処理部および電子署名生成部の一例を示したブロック図である。

【図５】証明書作成管理部、証明書作成処理部および電子署名生成部の他の例を示したブロック図である。

【図６】本発明の方法の全体フローを示したフローチャートである。

【図７】利用者がサービス要求をする場合の利用申請ダイアログの一例を示す表示図である。

【図８】利用者確認ステップの詳細を示したフローチャートである。

【図９】利用者要求を解析するステップの詳細を示したフローチャートである。

【図１０】登録者選出のステップの詳細を示したフローチャートである。

【図１１】証明作業の詳細を示したフローチャートである。

【図１２】証人作業を行う意思確認のダイアログの一例を示した表示図である。

【図１３】（ａ）は、時計同期の際に用いられる外部時計のシステムを表すブロック図であり、（ｂ）は、時計同期の方法を示すフローチャートである。

【図１４】（ａ）は、内部時計を利用して時刻同期を図るシステムを表すブロック図であり、（ｂ）は、方法を示すフローチャートである。

【図１５】証明書作成のステップを詳細に示したフローチャートである。

【図１６】電子署名を施す前段階の証明書作成ダイアログを示す表示画面図である。

【図１７】電子署名のステップを詳細に示したフローチャートである。

【図１８】証明書受理作業のステップを詳細に示したフローチャートである。

【図１９】サービス機関により作成された最終的な証明書の一例を示した表示画面図である。

【図２０】サービス機関により作成された最終的な証明書の他の例を示した表示画面図である。

【図２１】証明書発送作業のステップを詳細に示したフローチャートである。

【図２２】（ａ）は、証人登録のシステムを示すブロック図であり、（ｂ）は、その方法を示すフローチャートである。

【図２３】本発明の他の実施の形態（実施の形態２）である証明システムの一例を示した概念図である。

【図２４】実施の形態２のシステムのサービス機関および証明書生成器の一例を示したブロック図である。

【図２５】証明書作成管理部および証明書作成処理部の一例を示したブロック図である。

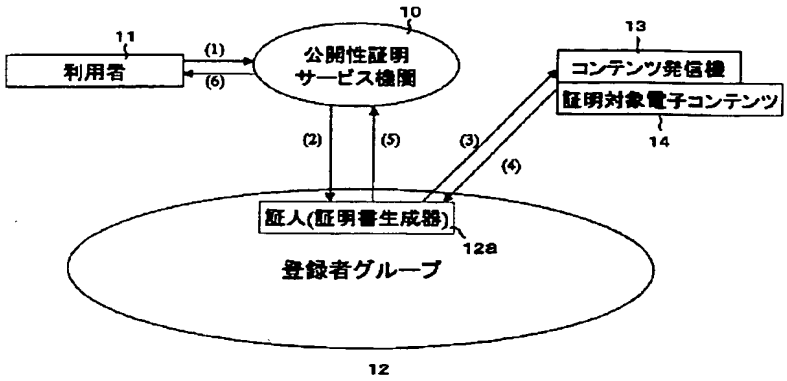
【図２６】本発明の証明システムの他の一例を示した概念図である。

【図２７】本発明の証明システムのさらに他の一例を示した概念図である。

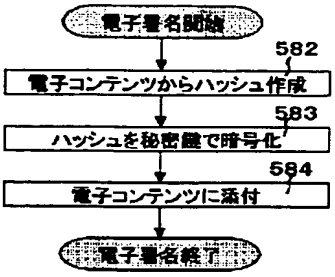
【符号の説明】

１０…サービス機関、１１…利用者、１２…登録者グループ、１２ａ…証人、１２ａ…証明書生成器、１３…コンテンツ発信機、１４…電子コンテンツ、２１…証明要求受信部、２２…証明書送信部、２３…証明作業管理部、２３ａ…時刻同期処理部、２４…通信部、２５…登録者選出部、２６…登録者データベース、２７…時計、２８…電子コンテンツ取得部、２９…通信部、３０…証明書作成管理部、３１…電子コンテンツ取得部、３２…時計（内部時計）、３３…証明書作成処理部、３４…電子署名生成部、３６…公開鍵認証サーバ、４０…登録者データベース、４１…証人登録管理部、４２…通信部、４３…通信部、４４…証人登録部、８１…ボタン、２１１…利用者アドレス、２１２…コンテンツアドレス、２１３…証人条件、２１４…証明機関、２１５…証明精度、２３１…利用者確認部、２３２…利用者要求解析部、２３３…利用履歴ファイル、２３４…証明書発送部、２３５…証明書受理部、２３７…時刻管理部、３０２…電子コンテンツ、３０３…時刻、３３１…データ、３３２…証明書、３４１…ハッシュ関数器、３４２…ハッシュコード、３４３…秘密鍵暗号化手段、３４４…暗号化ハッシュコード、３４５…公開鍵、３４６…暗号化コンテンツアドレス、３４７…暗号化電子コンテンツ、３４８…暗号化時刻、８００…ダイアログ、８００…入力ダイアログ、８０１…入力フィールド、８０２～８０９…入力フィールド、８１０…ボタン、８２０…ダイアログ、８２１…ボタン、８２２…ボタン、８３０…ダイアログ、８３１…フィールド、８３２…表示フィールド、８３４…ボタン、８３５…ボタン、８４０…フレーム、８４１…フィールド、８４２…フィールド、８４３…フィールド、８５０…フレーム、８５１…フィールド、８５２～８５５…フィールド、８５６…フィールド、９００…公証人サービス機関（電子公証サービス機関）、９０１…証人プロファイル、９０２…データ、９０３…証明書。

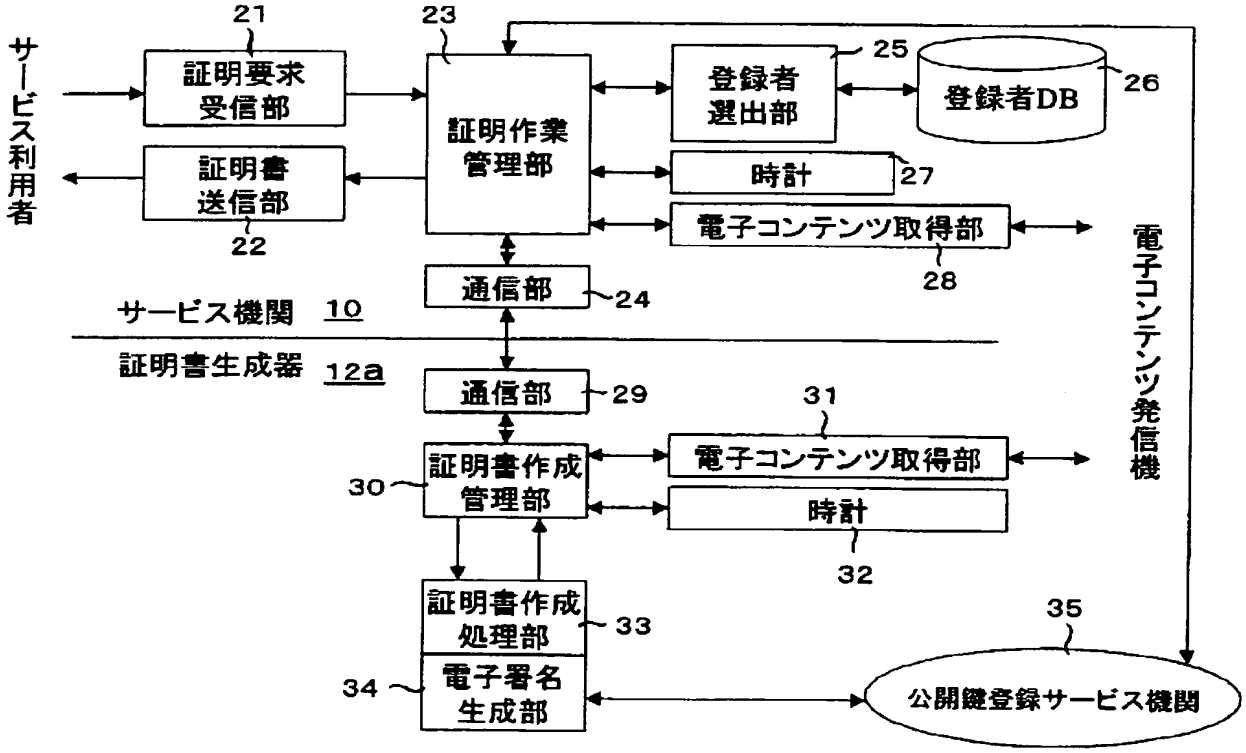
【図１】


10
11
利用者
(1)
(6)
公開性証明
サービス機関
13
コンテンツ発信機
証明対象電子コンテンツ
14
(2)
(5)
(3)
(4)
証人(証明書生成器)
12a
登録者グループ
12

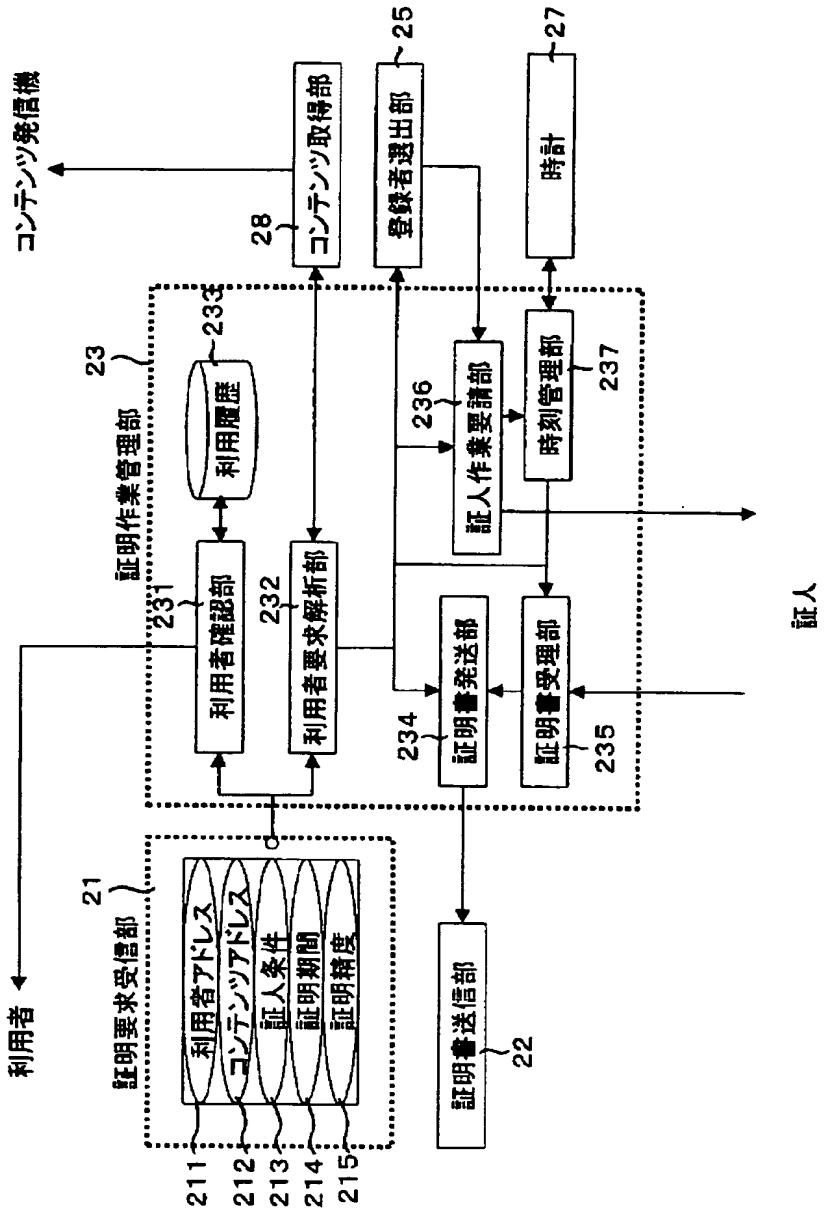
【図１７】


電子署名開始
582
電子コンテンツからハッシュ作成
583
ハッシュを秘密鍵で暗号化
584
電子コンテンツに添付
電子署名終了

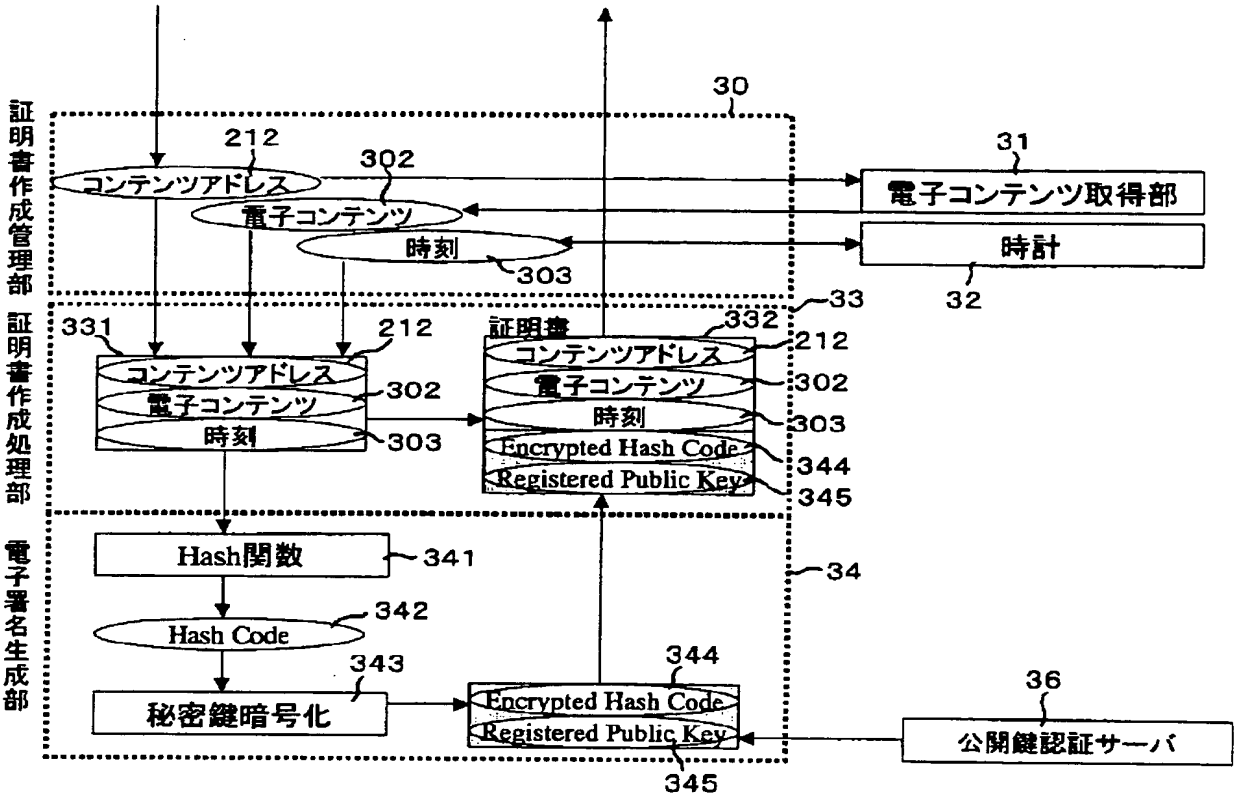
【図２】


サービス利用者
21
証明要求
受信部
証明書
送信部
22
23
証明作業
管理部
25
登録者
選出部
登録者DB
26
時計
27
電子コンテンツ取得部
28
通信部
24
サービス機関 10
証明書生成器 12a
通信部
29
31
証明書作成
管理部
30
電子コンテンツ取得部
時計
32
証明書作成
処理部
33
電子署名
生成部
34
35
公開鍵登録サービス機関
電子コンテンツ発信機

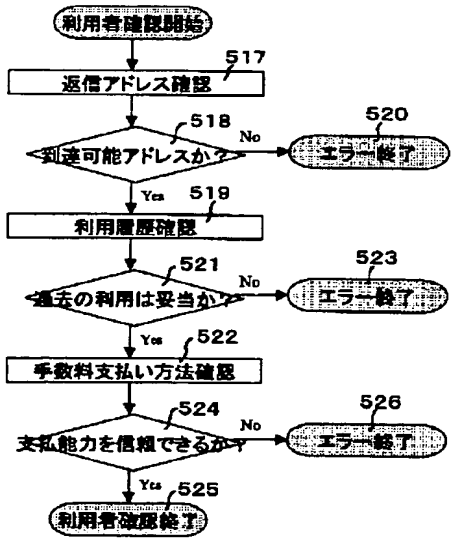
【図３】


コンテンツ発信機
利用者
証人
証明要求受信部
21
利用者アドレス
コンテンツアドレス
証人条件
証明期間
証明精度
211
212
213
214
215
証明作業管理部
23
利用者確認部
231
利用者要求解析部
232
利用履歴
233
コンテンツ取得部
28
登録者選出部
25
時計
27
証人作業要請部
236
時刻管理部
237
証明書発送部
234
証明書受理部
235
証明書送信部
22

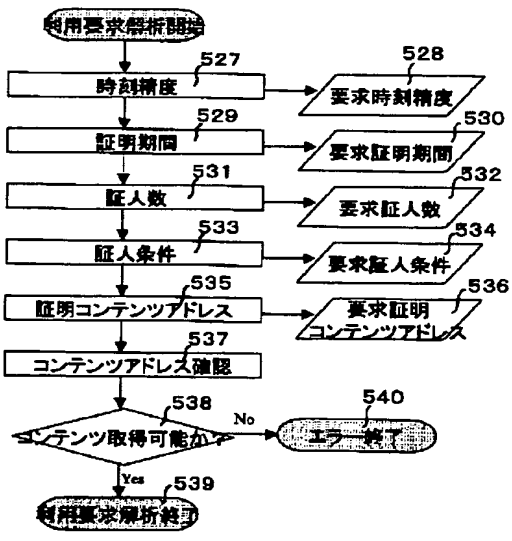
【図４】


証明書作成管理部
証明書作成処理部
電子署名生成部
30
31
32
33
34
212
302
303
331
332
341
342
343
344
345
36
コンテンツアドレス
電子コンテンツ
時刻
電子コンテンツ取得部
時計
証明書
Encrypted Hash Code
Registered Public Key
Hash関数
Hash Code
秘密鍵暗号化
公開鍵認証サーバ

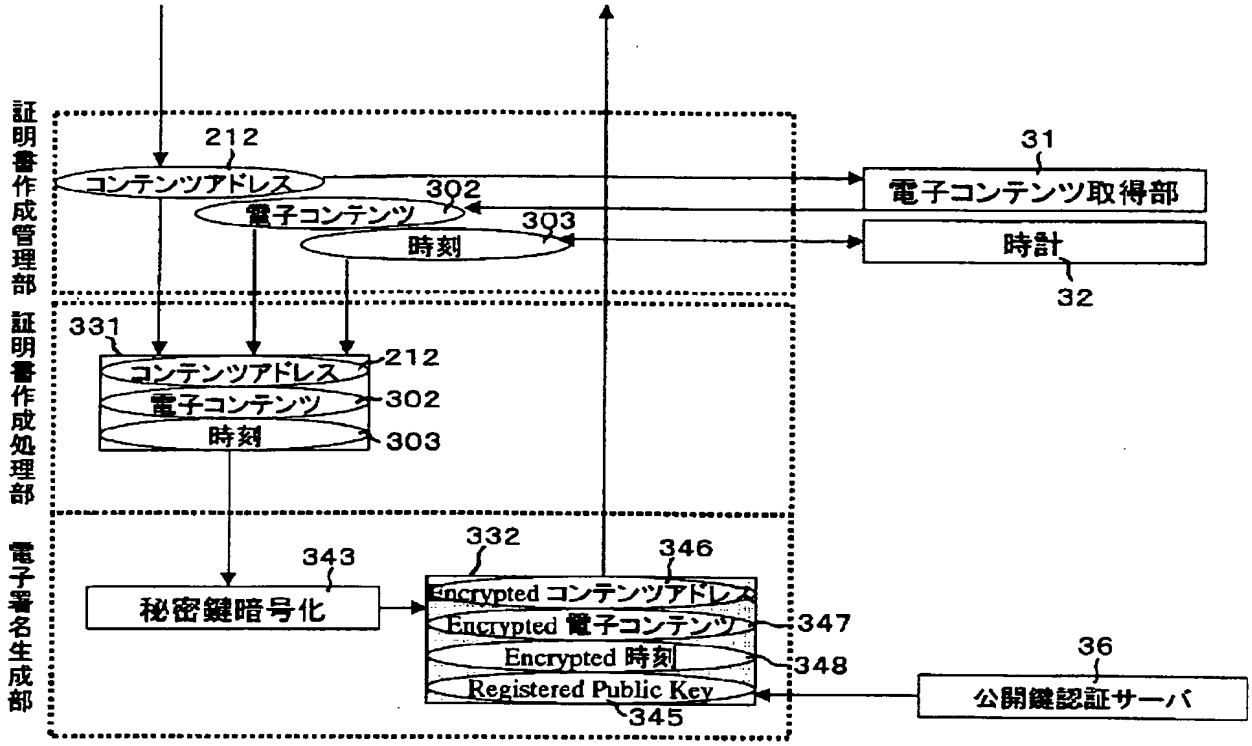
【図８】


利用者確認開始
返信アドレス確認
517
到達可能アドレスか？
518
No
520
エラー終了
Yes
利用履歴確認
519
過去の利用は妥当か？
521
No
523
エラー終了
Yes
手数料支払い方法確認
522
支払能力を信頼できるか？
524
No
526
エラー終了
Yes
利用者確認終了
525

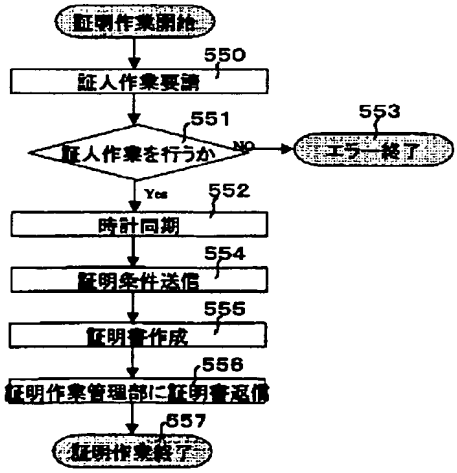
【図９】


利用要求解析開始
時刻精度
527
528
要求時刻精度
証明期間
529
530
要求証明期間
証人数
531
532
要求証人数
証人条件
533
534
要求証人条件
証明コンテンツアドレス
535
536
要求証明コンテンツアドレス
コンテンツアドレス確認
537
コンテンツ取得可能か？
538
No
540
エラー終了
Yes
利用要求解析終了
539

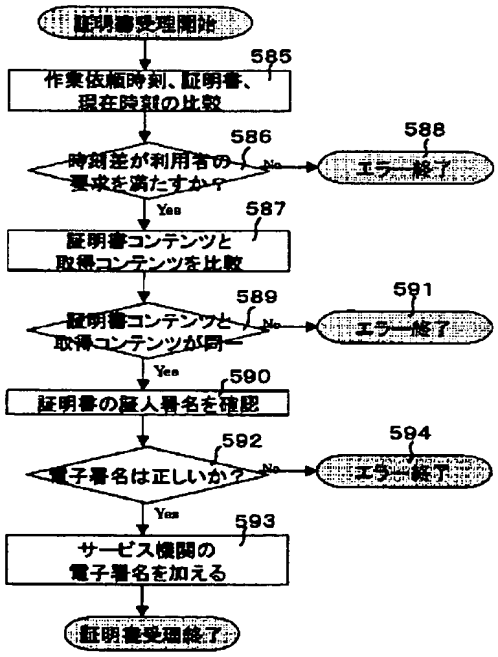
【図５】


証明書作成管理部
証明書作成処理部
電子署名生成部
212
コンテンツアドレス
302
電子コンテンツ
303
時刻
31
電子コンテンツ取得部
時計
32
331
コンテンツアドレス
212
電子コンテンツ
302
時刻
303
343
秘密鍵暗号化
332
346
Encrypted コンテンツアドレス
Encrypted 電子コンテンツ
347
Encrypted 時刻
348
Registered Public Key
345
36
公開鍵認証サーバ

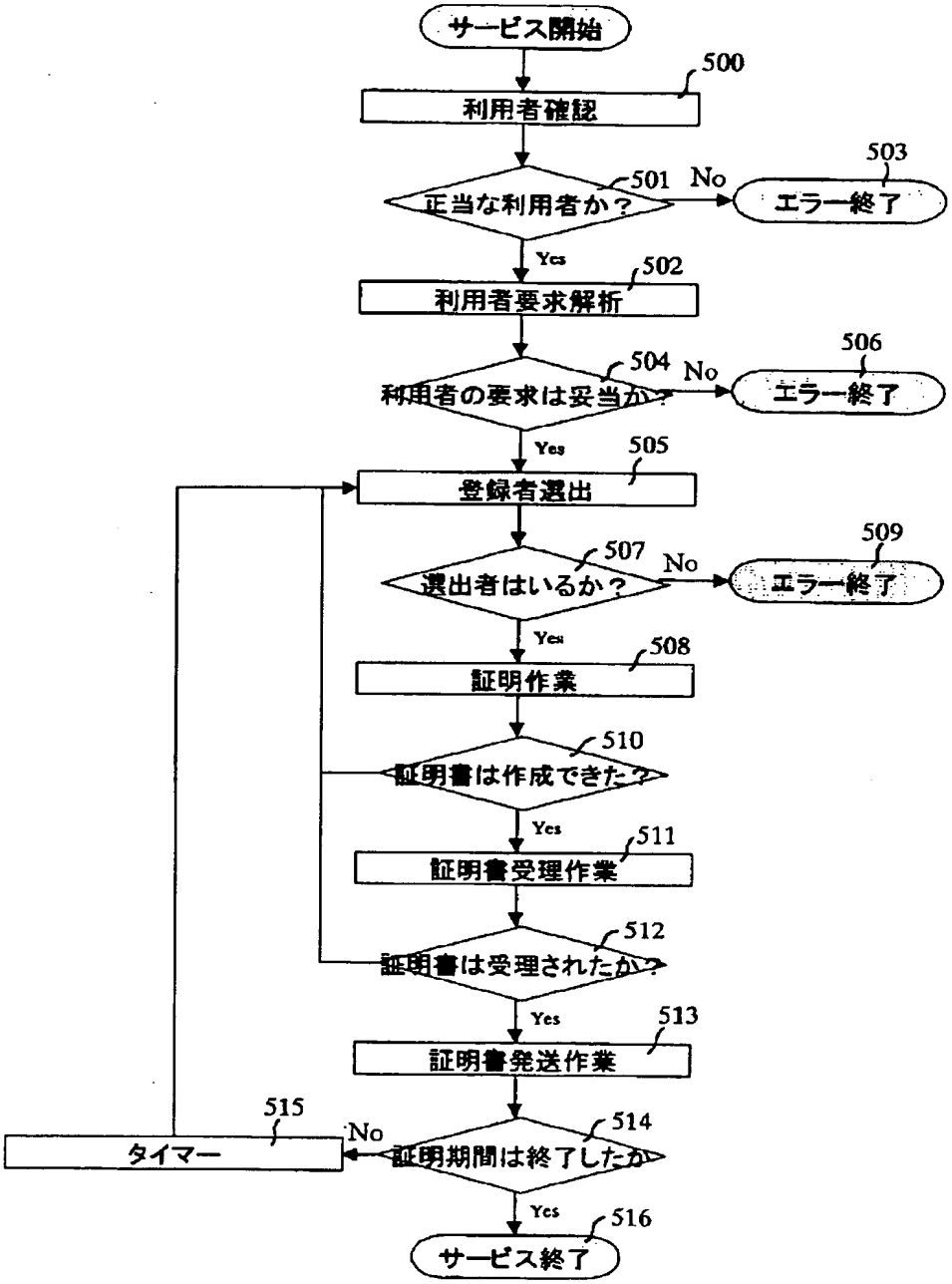
【図１１】


証明作業開始
550
証人作業要請
551
証人作業を行うか
No
553
エラー終了
Yes
552
時計同期
554
証明条件送信
555
証明書作成
556
証明作業管理部に証明書返信
557
証明作業終了

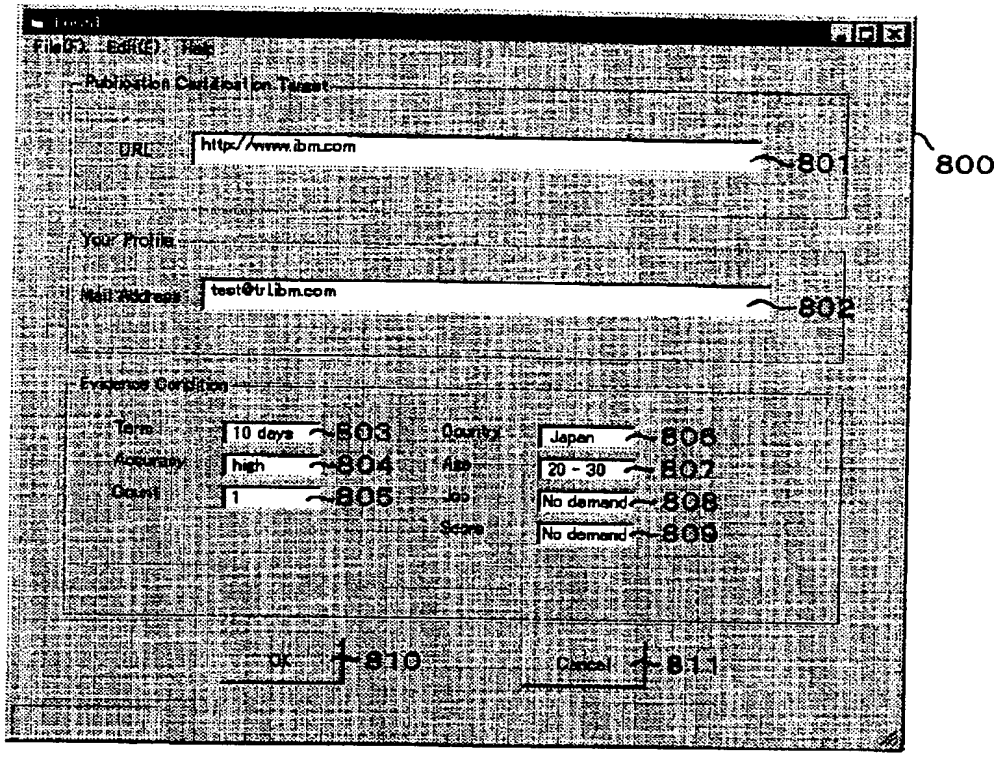
【図１８】


証明書受理開始
585
作業依頼時刻、証明書、現在時刻の比較
586
時刻差が利用者の要求を満たすか？
No
588
エラー終了
Yes
587
証明書コンテンツと取得コンテンツを比較
589
証明書コンテンツと取得コンテンツが同一
No
591
エラー終了
Yes
590
証明書の証人署名を確認
592
電子署名は正しいか？
No
594
エラー終了
Yes
593
サービス機関の電子署名を加える
証明書受理終了

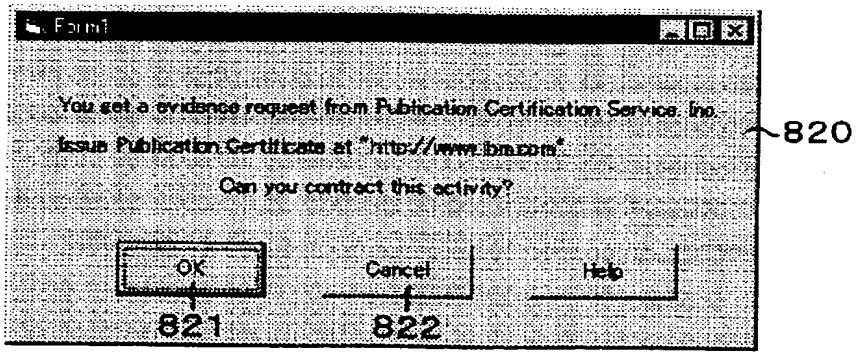
【図６】


サービス開始
500
利用者確認
501
正当な利用者か？
No
503
エラー終了
Yes
502
利用者要求解析
504
利用者の要求は妥当か？
No
506
エラー終了
Yes
505
登録者選出
507
選出者はいるか？
No
509
エラー終了
Yes
508
証明作業
510
証明書は作成できた？
Yes
511
証明書受理作業
512
証明書は受理されたか？
Yes
513
証明書発送作業
514
証明期間は終了したか
No
515
タイマー
Yes
516
サービス終了

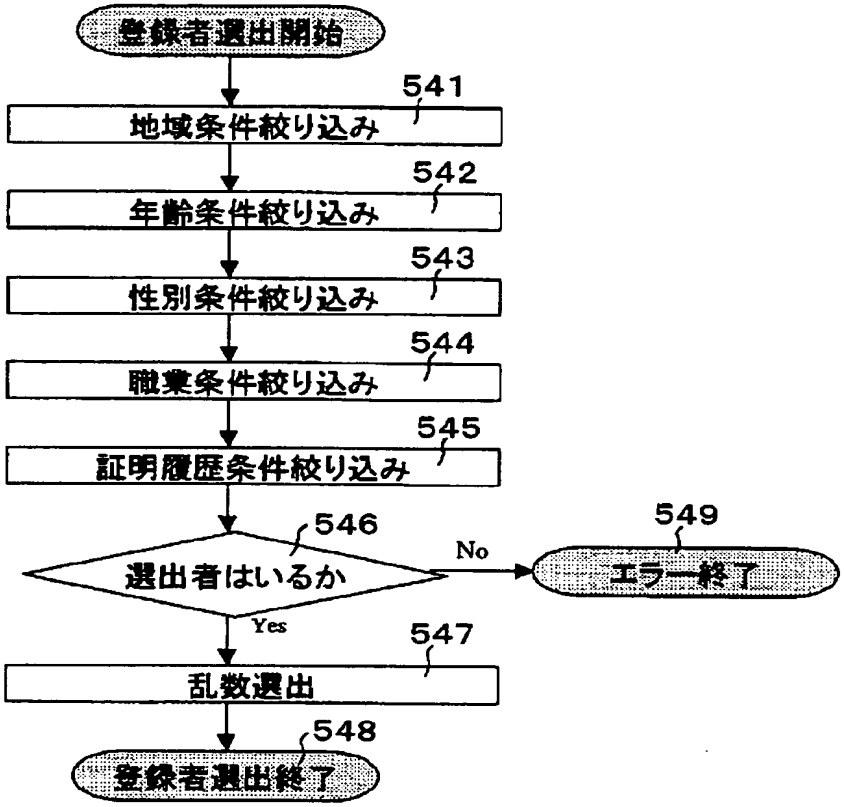
【図７】


File(F) Edit(E) Help
Publication Certification Tester
URL
http://www.ibm.com
801
800
Your Profile
Mail Address
test@trlibm.com
802
Evidence Condition
Term
10 days
803
Country
Japan
806
Accuracy
high
804
Age
20 - 30
807
Num
1
805
Job
No demand
808
Scope
No demand
809
OK
810
Cancel
811

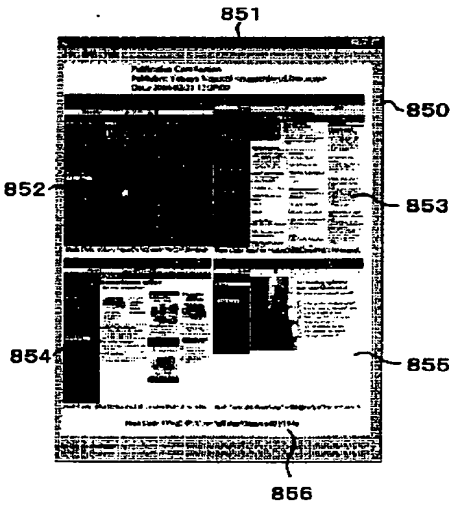
【図１２】


Form1
You set a evidence request from Publication Certification Service, Inc.
Issue Publication Certificate at "http://www.ibm.com".
Can you contract this activity?
820
OK
Cancel
Help
821
822

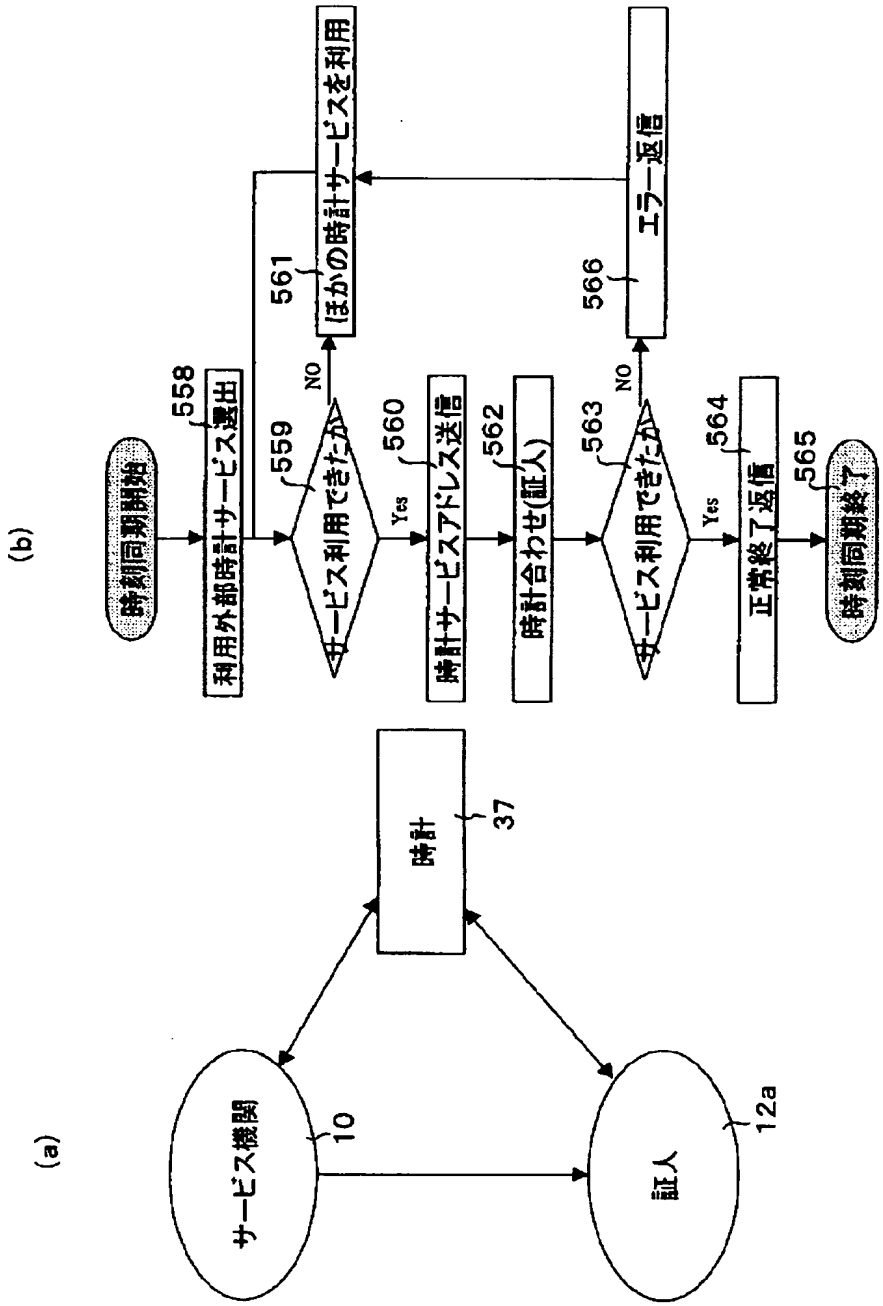
【図１０】


登録者選出開始
541
地域条件絞り込み
542
年齢条件絞り込み
543
性別条件絞り込み
544
職業条件絞り込み
545
証明履歴条件絞り込み
546
選出者はいるか
No
549
エラー終了
Yes
547
乱数選出
548
登録者選出終了

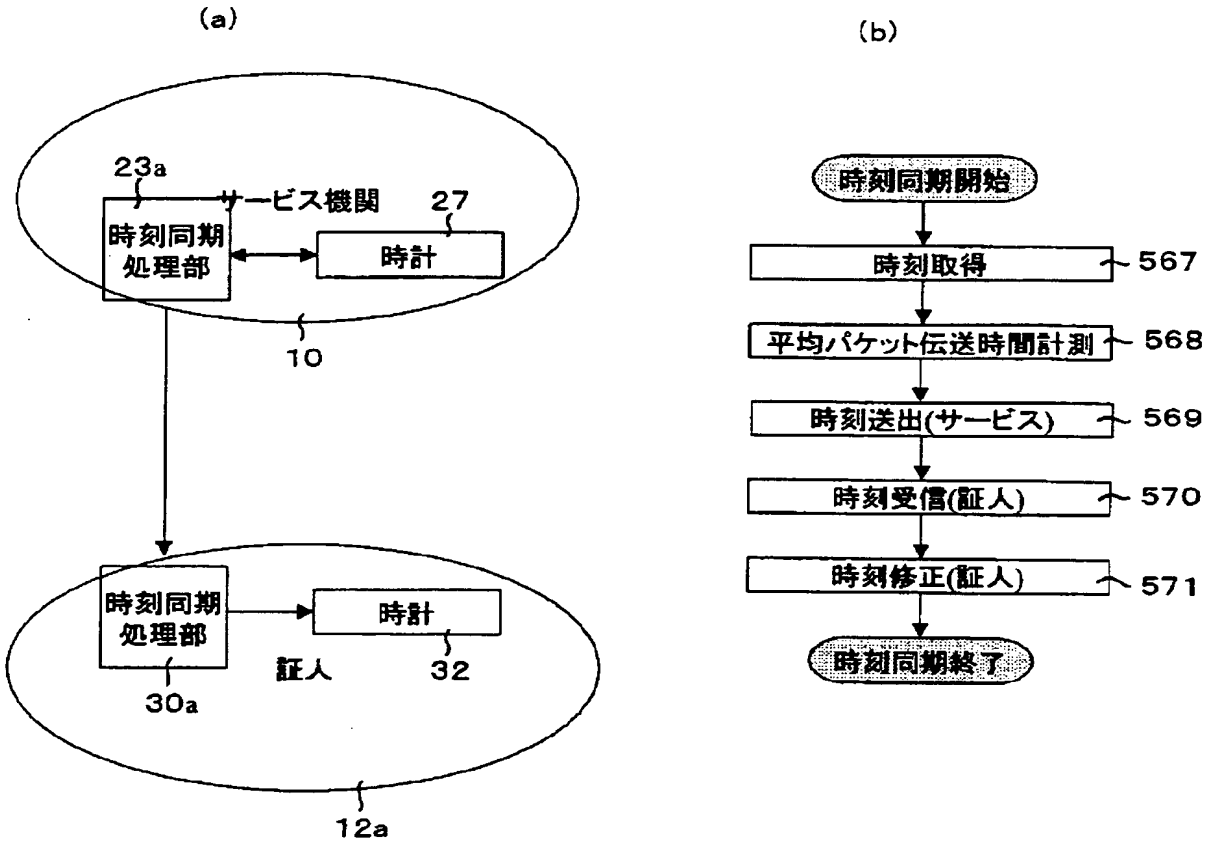
【図２０】


851
850
852
853
854
855
856

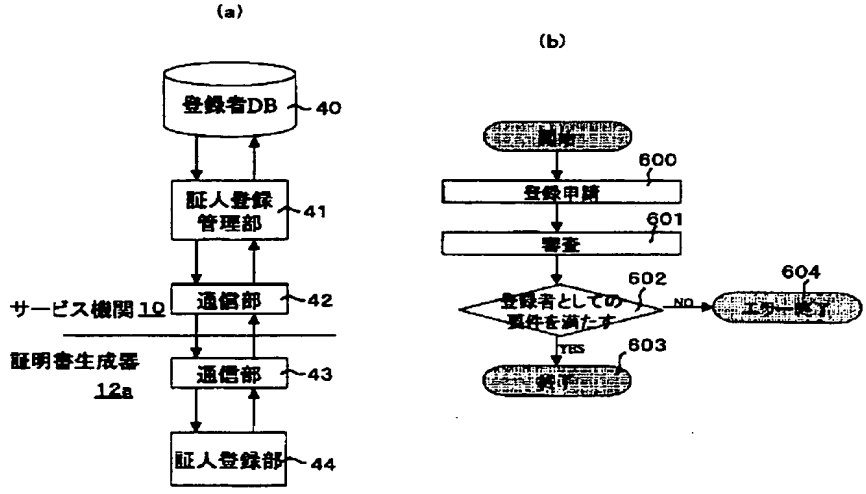
【図１３】


(a)
サービス機関
10
時計
37
証人
12a
(b)
時刻同期開始
利用外部時計サービス選出
558
サービス利用できたか
559
NO
ほかの時計サービスを利用
561
Yes
時計サービスアドレス送信
560
時計合わせ(証人)
562
サービス利用できたか
563
NO
エラー返信
566
Yes
正常終了返信
564
時刻同期終了
565

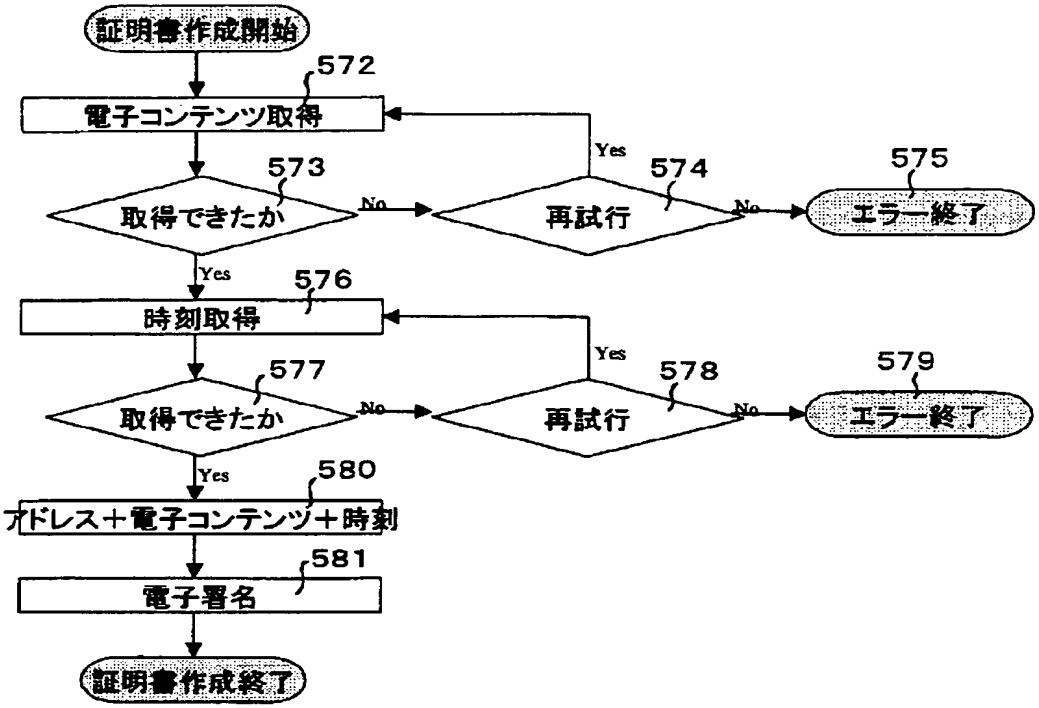
【図１４】


(a)
23a
サービス機関
27
時刻同期処理部
時計
10
時刻同期処理部
時計
証人
32
30a
12a
(b)
時刻同期開始
時刻取得
567
平均パケット伝送時間計測
568
時刻送出(サービス)
569
時刻受信(証人)
570
時刻修正(証人)
571
時刻同期終了

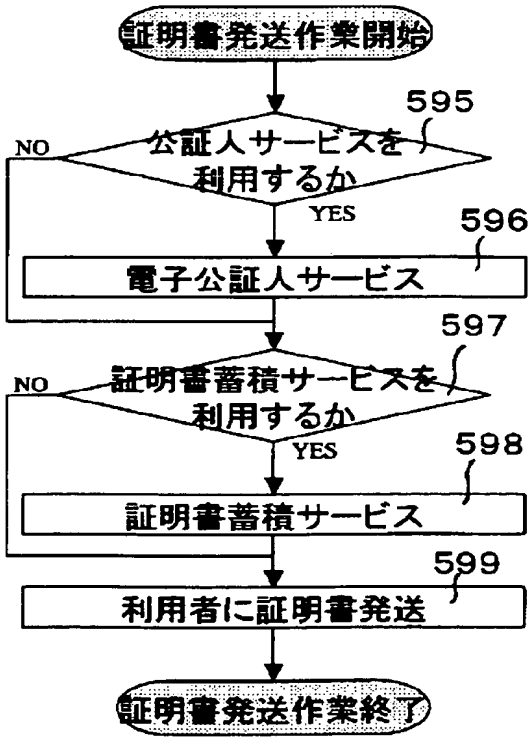
【図２２】


(a)
登録者DB
40
証人登録管理部
41
サービス機関10
通信部
42
証明書生成器12a
通信部
43
証人登録部
44
(b)
開始
600
登録申請
601
審査
602
登録者としての要件を満たす
NO
604
エラー終了
YES
603
終了

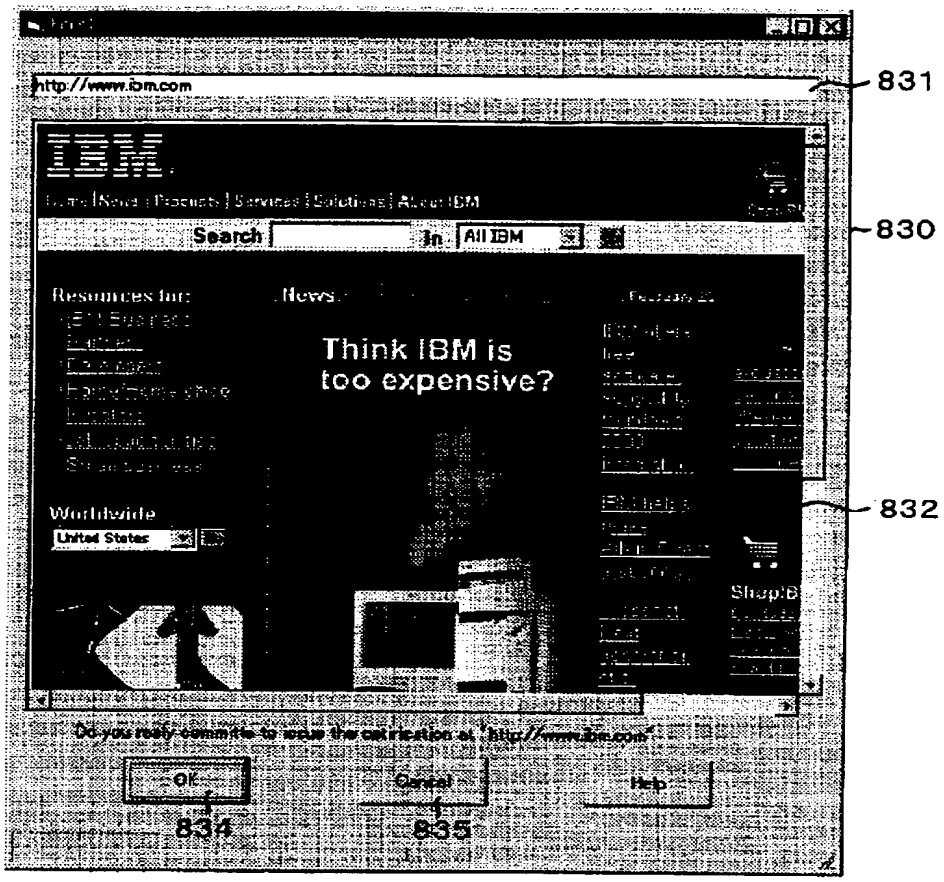
【図１５】


証明書作成開始
572
電子コンテンツ取得
573
取得できたか
No
Yes
574
再試行
No
Yes
575
エラー終了
576
時刻取得
577
取得できたか
No
Yes
578
再試行
No
Yes
579
エラー終了
580
アドレス＋電子コンテンツ＋時刻
581
電子署名
証明書作成終了

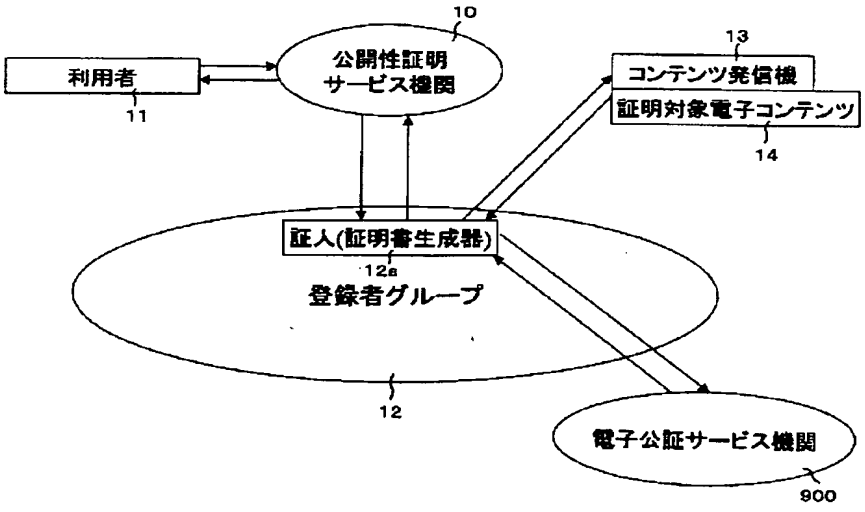
【図２１】


証明書発送作業開始
595
公証人サービスを利用するか
NO
YES
596
電子公証人サービス
597
証明書蓄積サービスを利用するか
NO
YES
598
証明書蓄積サービス
599
利用者に証明書発送
証明書発送作業終了

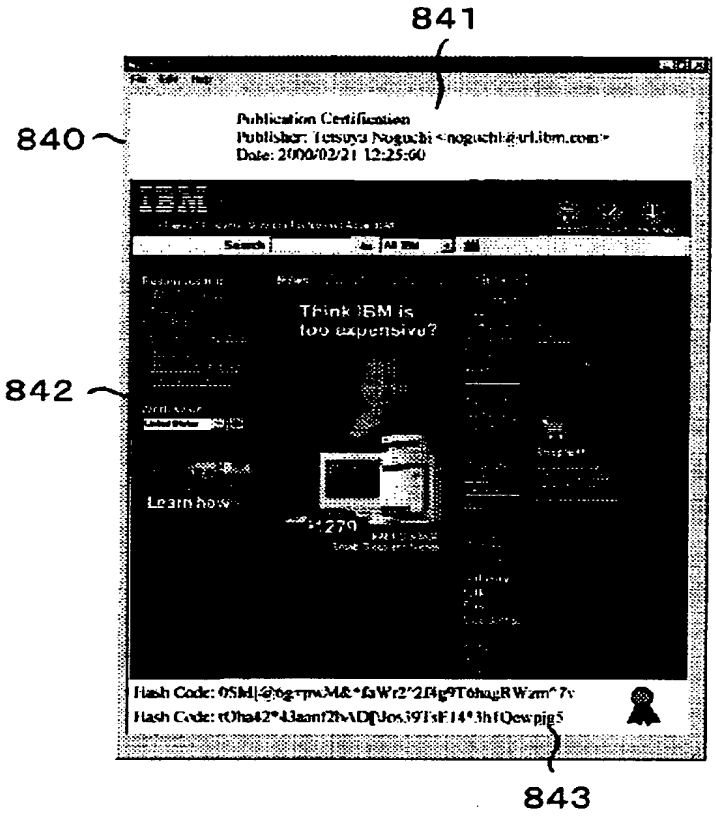
【図１６】


http://www.ibm.com
831
IBM
Search
In
All IBM
830
Resources for:
News:
Think IBM is
too expensive?
Worldwide
United States
832
Shop:B
Do you really commite to wiew the ontriction at 'http://www.ibm.com'
OK
Cancel
Help
834
835

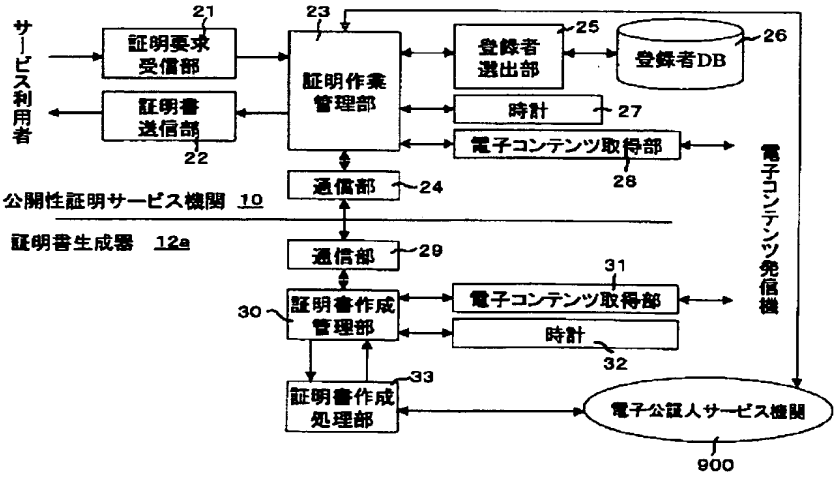
【図２３】


10
利用者
11
公開性証明
サービス機関
13
コンテンツ発信機
証明対象電子コンテンツ
14
証人(証明書生成器)
12a
登録者グループ
12
電子公証サービス機関
900

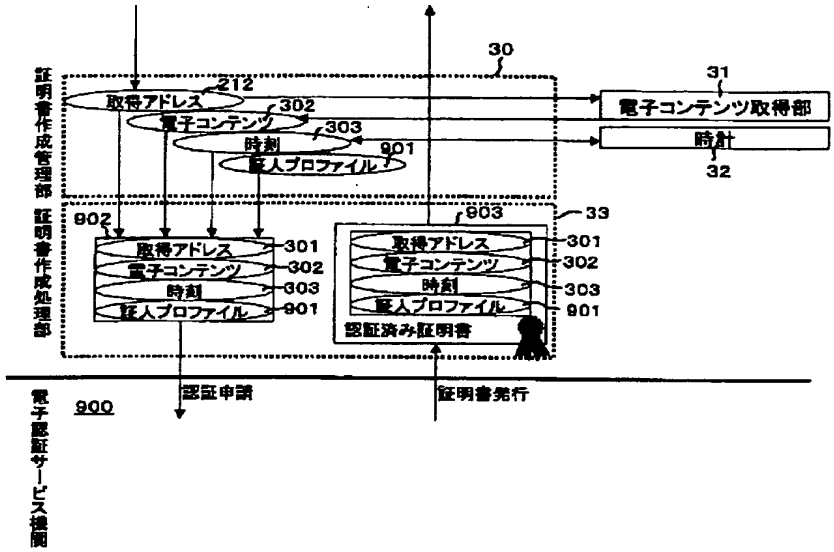
【図１９】


841
840
Publication Certification
Publisher: Tetsuya Noguchi <noguchi@url.ibm.com>
Date: 2000/02/21 12:25:60
842
Think IBM is too expensive?
Learn how
843

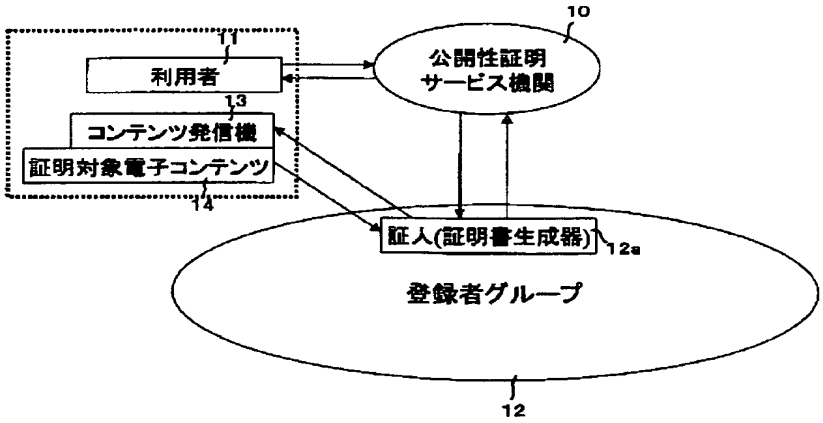
【図２４】


サービス利用者
21
証明要求受信部
22
証明書送信部
23
証明作業管理部
24
通信部
25
登録者選出部
26
登録者DB
27
時計
28
電子コンテンツ取得部
電子コンテンツ発信機
公開性証明サービス機関 10
証明書生成器 12a
29
通信部
30
証明書作成管理部
31
電子コンテンツ取得部
32
時計
33
証明書作成処理部
電子公証人サービス機関
900

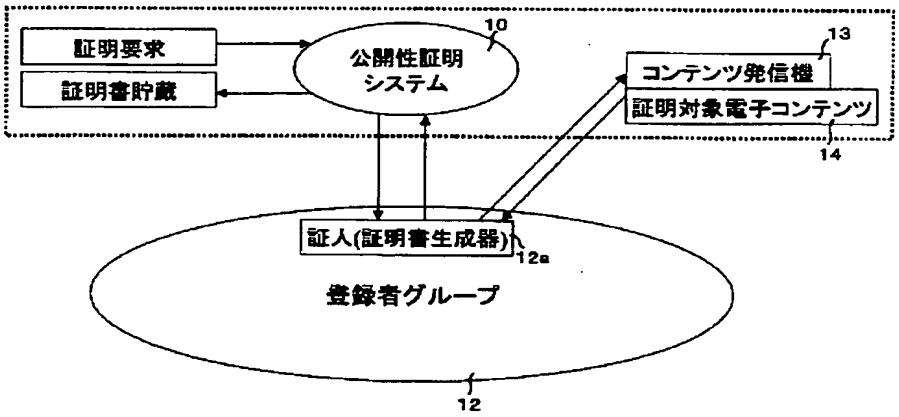
【図２５】


30
31
212
取得アドレス
302
電子コンテンツ
303
時刻
901
証人プロファイル
電子コンテンツ取得部
時計
32
証明書作成管理部
902
903
33
取得アドレス
301
電子コンテンツ
302
時刻
303
証人プロファイル
901
認証済み証明書
証明書作成処理部
認証申請
証明書発行
900
電子認証サービス機関

【図２６】


10
11
利用者
公開性証明
サービス機関
13
コンテンツ発信機
証明対象電子コンテンツ
14
証人(証明書生成器)
12a
登録者グループ
12

【図２７】



フロントページの続き

(72)発明者　野口　哲也
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内

(72)発明者　小柳　光生
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内

(72)発明者　鹿島　久嗣
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内

Ｆターム(参考)　5B085 AC05 AE09 AE13 AE23 BG07 CA04
5J104 AA09 EA01 GA03 JA21 LA06 MA01 NA02 NA12 NA27 PA07
9A001 BB03 BB04 EE03 GG21 JJ25 JJ27 KK56 LL03 LL09